07.04.00

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

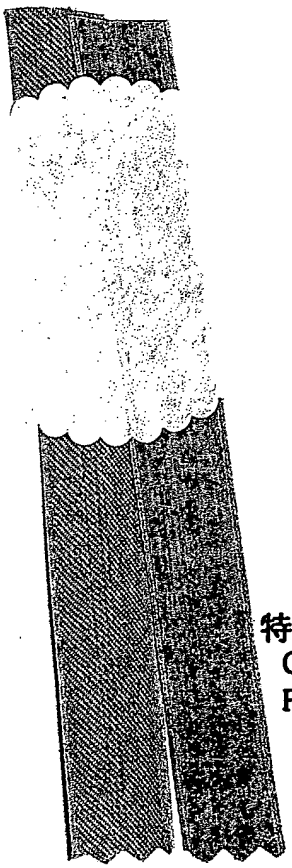
EKV

出 願 年 月 日
Date of Application: １９９９年 ４月 ９日

出 願 番 号
Application Number: 平成１１年特許願第１０３３３９号

出 願 人
Applicant (s): ソニー株式会社

09/719015



PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

CERTIFIED COPY OF PRIORITY DOCUMENT

２０００年 ５月１２日

特 許 庁 長 官
Commissioner,
Patent Office

近 藤 隆 彦

出証番号 出証特２０００－３０３４９６３

【書類名】　特許願

【整理番号】　9900015606

【提出日】　平成11年 4月 9日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 12/16

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　石橋　義人

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　浅野　智之

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　北村　出

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　北原　淳

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100082131

【弁理士】

【氏名又は名称】　稲本　義雄

【電話番号】　03-3369-6479

【手数料の表示】

【予納台帳番号】　032089

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9708842

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置および方法、並びに提供媒体

【特許請求の範囲】

【請求項１】　他の情報処理装置に接続され、かつ、管理装置に管理されて、暗号化された情報を復号して利用する情報処理装置において、

前記他の情報処理装置の所定の代理決済情報を記憶する記憶手段と、

前記記憶手段に記憶されている前記代理決済情報に対応して、所定の課金情報の提供を前記他の情報処理装置に要求する要求手段と、

前記要求手段による要求に応じて、前記他の情報処理装置から送信されてくる前記課金情報を受信する第１の受信手段と、

前記第１の受信手段により受信された前記課金情報を、前記管理装置に送信する送信手段と、

前記管理装置から送信されてくる、前記送信手段により送信された前記課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受信する第２の受信手段と、

前記第２の受信手段により受信された前記登録条件に基づいて、動作を制御する制御手段と

を備えることを特徴とする情報処理装置。

【請求項２】　他の情報処理装置に接続され、かつ、管理装置に管理されて、暗号化された情報を復号して利用する情報処理装置の情報処理方法において、

前記他の情報処理装置の所定の代理決済情報を記憶する記憶ステップと、

前記記憶ステップで記憶された前記代理決済情報に対応して、所定の課金情報の提供を前記他の情報処理装置に要求する要求ステップと、

前記要求ステップでの要求に応じて、前記他の情報処理装置から送信されてくる前記課金情報を受信する第１の受信ステップと、

前記第１の受信ステップで受信された前記課金情報を、前記管理装置に送信する送信ステップと、

前記管理装置から送信されてくる、前記送信ステップで送信された前記課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受

信する第２の受信ステップと、

前記第２の受信ステップで受信された前記登録条件に基づいて、動作を制御する制御ステップと

を含むことを特徴とする情報処理方法。

【請求項３】　他の情報処理装置に接続され、かつ、管理装置に管理されて、暗号化された情報を復号して利用する情報処理装置に、

前記他の情報処理装置の所定の代理決済情報を記憶する記憶ステップと、

前記記憶ステップで記憶された前記代理決済情報に対応して、所定の課金情報の提供を前記他の情報処理装置に要求する要求ステップと、

前記要求ステップでの要求に応じて、前記他の情報処理装置から送信されてくる前記課金情報を受信する第１の受信ステップと、

前記第１の受信ステップで受信された前記課金情報を、前記管理装置に送信する送信ステップと、

前記管理装置から送信されてくる、前記送信ステップで送信された前記課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受信する第２の受信ステップと、

前記第２の受信ステップで受信された前記登録条件に基づいて、動作を制御する制御ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項４】　他の情報処理装置に接続され、かつ、管理装置に管理されて、暗号化された情報を復号して利用する情報処理装置において、

前記他の情報処理装置の所定の代理購入情報を記憶する第１の記憶手段と、

前記第１の記憶手段に記憶されている前記代理購入情報に対応して、所定の課金情報を作成する第１の作成手段と、

前記第１の記憶手段に記憶されている前記代理購入情報に対応して、所定の使用許諾条件情報を作成する第２の作成手段と、

前記第１の作成手段により作成された前記課金情報を記憶する第２の記憶手段と、

前記第２の作成手段により作成された前記使用許諾条件情報と、前記管理装置から供給された、暗号化された前記情報を復号するために必要な鍵を、前記他の情報処理装置に送信する送信手段と

を備えることを特徴とする情報処理装置。

【請求項５】　前記他の情報処理装置が、

所定の表示を制御する表示手段と、

所定のデータの入力を制御する入力制御手段と

を備えているとき、

前記第１の作成手段は、前記表示手段により制御された前記表示が参照されて、前記入力制御手段に入力されたデータに基づいて、前記課金情報を作成し、

前記第２の作成手段は、前記表示手段により制御された前記表示が参照されて、前記入力制御手段に制御された前記データに基づいて、前記使用許諾条件情報を作成する

ことを特徴とする請求項４に記載の情報処理装置。

【請求項６】　他の情報処理装置に接続され、かつ、管理装置に管理されて、暗号化された情報を復号して利用する情報処理装置の情報処理方法において、

前記他の情報処理装置の所定の代理購入情報を記憶する第１の記憶ステップと、

前記第１の記憶ステップで記憶された前記代理購入情報に対応して、所定の課金情報を作成する第１の作成ステップと、

前記第１の記憶ステップで記憶された前記代理購入情報に対応して、所定の使用許諾条件情報を作成する第２の作成ステップと、

前記第１の作成ステップで作成された前記課金情報を記憶する第２の記憶ステップと、

前記第２の作成ステップで作成された前記使用許諾条件情報と、前記管理装置から供給された、暗号化された前記情報を復号するために必要な鍵を、前記他の情報処理装置に送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項７】　他の情報処理装置に接続され、かつ、管理装置に管理されて

、暗号化された情報を復号して利用する情報処理装置に、

前記他の情報処理装置の所定の代理購入情報を記憶する第１の記憶ステップと、

前記第１の記憶ステップで記憶された前記代理購入情報に対応して、所定の課金情報を作成する第１の作成ステップと、

前記第１の記憶ステップで記憶された前記代理購入情報に対応して、所定の使用許諾条件情報を作成する第２の作成ステップと、

前記第１の作成ステップで作成された前記課金情報を記憶する第２の記憶ステップと、

前記第２の作成ステップで作成された前記使用許諾条件情報と、前記管理装置から供給された、暗号化された前記情報を復号するために必要な鍵を、前記他の情報処理装置に送信する送信ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置および方法、並び提供媒体に関し、特に、暗号化された情報を利用する情報処理装置および方法、並びに提供媒体に関する。

【０００２】

【従来の技術】

音楽などの情報（以下、コンテンツと称する）を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザが、情報処理装置でコンテンツを復号して、利用するシステムがある。

【０００３】

【発明が解決しようとする課題】

複数の情報処理装置を有している場合、ユーザは、それぞれの情報処理装置毎に、コンテンツを購入し、その利用料金を精算しなければならず、手間がかかる課題があった。

【０００４】

本発明はこのような状況に鑑みてなされたものであり、ユーザが複数の情報処理装置を有している場合、主とする情報処理装置を利用して、他の情報処理装置で利用されるコンテンツを購入したり、料金の精算をすることができるようにするものである。

【０００５】

【課題を解決するための手段】

請求項１に記載の情報処理装置は、他の情報処理装置の所定の代理決済情報を記憶する記憶手段と、記憶手段に記憶されている代理決済情報に対応して、所定の課金情報の提供を他の情報処理装置に要求する要求手段と、要求手段による要求に応じて、他の情報処理装置から送信されてくる課金情報を受信する第１の受信手段と、第１の受信手段により受信された課金情報を、管理装置に送信する送信手段と、管理装置から送信されてくる、送信手段により送信された課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受信する第２の受信手段と、第２の受信手段により受信された登録条件に基づいて、動作を制御する制御手段とを備えることを特徴とする。

【０００６】

請求項２に記載の情報処理方法は、他の情報処理装置の所定の代理決済情報を記憶する記憶ステップと、記憶ステップで記憶された代理決済情報に対応して、所定の課金情報の提供を他の情報処理装置に要求する要求ステップと、要求ステップでの要求に応じて、他の情報処理装置から送信されてくる課金情報を受信する第１の受信ステップと、第１の受信ステップで受信された課金情報を、管理装置に送信する送信ステップと、管理装置から送信されてくる、送信ステップで送信された課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受信する第２の受信ステップと、第２の受信ステップで受信された登録条件に基づいて、動作を制御する制御ステップとを含むことを特徴とする。

【０００７】

請求項３に記載の提供媒体は、他の情報処理装置の所定の代理決済情報を記憶する記憶ステップと、記憶ステップで記憶された代理決済情報に対応して、所定

の課金情報の提供を他の情報処理装置に要求する要求ステップと、要求ステップでの要求に応じて、他の情報処理装置から送信されてくる課金情報を受信する第１の受信ステップと、第１の受信ステップで受信された課金情報を、管理装置に送信する送信ステップと、管理装置から送信されてくる、送信ステップで送信された課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受信する第２の受信ステップと、第２の受信ステップで受信された登録条件に基づいて、動作を制御する制御ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【０００８】

請求項１に記載の情報処理装置、請求項２に記載の情報処理方法、および請求項３に記載の提供媒体においては、他の情報処理装置の所定の代理決済情報が記憶され、記憶された代理決済情報に対応して、所定の課金情報の提供が他の情報処理装置に要求され、要求に応じて、他の情報処理装置から送信されてくる課金情報が受信され、受信された課金情報が、管理装置に送信され、管理装置から送信されてくる、送信された課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件が受信され、受信された登録条件に基づいて、動作が制御される。

【０００９】

請求項４に記載の情報処理装置は、他の情報処理装置の所定の代理購入情報を記憶する第１の記憶手段と、第１の記憶手段に記憶されている代理購入情報に対応して、所定の課金情報を作成する第１の作成手段と、第１の記憶手段に記憶されている代理購入情報に対応して、所定の使用許諾条件情報を作成する第２の作成手段と、第１の作成手段により作成された課金情報を記憶する第２の記憶手段と、第２の作成手段により作成された使用許諾条件情報と、管理装置から供給された、暗号化された情報を復号するために必要な鍵を、他の情報処理装置に送信する送信手段とを備えることを特徴とする。

【００１０】

請求項６に記載の情報処理方法は、他の情報処理装置の所定の代理購入情報を記憶する第１の記憶ステップと、第１の記憶ステップで記憶された代理購入情報

に対応して、所定の課金情報を作成する第１の作成ステップと、第１の記憶ステップで記憶された代理購入情報に対応して、所定の使用許諾条件情報を作成する第２の作成ステップと、第１の作成ステップで作成された課金情報を記憶する第２の記憶ステップと、第２の作成ステップで作成された使用許諾条件情報と、管理装置から供給された、暗号化された情報を復号するために必要な鍵を、他の情報処理装置に送信する送信ステップとを含むことを特徴とする。

【００１１】

請求項７に記載の提供媒体は、他の情報処理装置の所定の代理購入情報を記憶する第１の記憶ステップと、第１の記憶ステップで記憶された代理購入情報に対応して、所定の課金情報を作成する第１の作成ステップと、第１の記憶ステップで記憶された代理購入情報に対応して、所定の使用許諾条件情報を作成する第２の作成ステップと、第１の作成ステップで作成された課金情報を記憶する第２の記憶ステップと、第２の作成ステップで作成された使用許諾条件情報と、管理装置から供給された、暗号化された情報を復号するために必要な鍵を、他の情報処理装置に送信する送信ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【００１２】

請求項４に記載の情報処理装置、請求項６に記載の情報処理方法、および請求項７に記載の提供媒体においては、他の情報処理装置の所定の代理購入情報が記憶され、記憶されている代理購入情報に対応して、所定の課金情報が作成され、記憶されている代理購入情報に対応して、所定の使用許諾条件情報が作成され、作成された課金情報が記憶され、作成された使用許諾条件情報と、管理装置から供給された、暗号化された情報を復号するために必要な鍵を、他の情報処理装置に送信する送信手段とを備えることを特徴とする。

【００１３】

【発明の実施の形態】

以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次

のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【００１４】

図１は、本発明を適用したEMD(Electronic Music Distribution:電子音楽配信)システムを説明する図である。EMDシステムは、各装置を管理するEMDサービスセンタ１、コンテンツを提供するコンテンツプロバイダ２、コンテンツに対応する所定のサービスを提供するサービスプロバイダ３、およびコンテンツが利用される機器（この例の場合、HDD５２に接続されているレシーバ５１およびHDD２０２に接続されているレシーバ２０１）からなるユーザネットワーク５から構成されている。

【００１５】

EMDシステムにおけるコンテンツ(Content)とは、情報そのものが価値を有するデジタルデータで、この例の場合、１つのコンテンツは、１曲分の音楽データに相当する。

【００１６】

EMDサービスセンタ１は、EMDシステムにおける主な情報の流れを示す図２に示すように、ユーザホームネットワーク５およびコンテンツプロバイダ２に、コンテンツを利用するために必要な配送用鍵Ｋｄを送信する。EMDサービスセンタ１はまた、ユーザホームネットワーク５の機器から、課金情報等を受信して、料金を精算する処理などを実行する。

【００１７】

コンテンツプロバイダ２は、提供するコンテンツ（コンテンツ鍵Ｋｃｏで暗号化されている）、そのコンテンツを復号するために必要なコンテンツ鍵Ｋｃｏ（配送用鍵Ｋｄで暗号化されている）、およびコンテンツの利用内容などを示す取扱方針（以下、UCP(Usage Control Policy)と記述する）を保持し、それらを、コンテンツプロバイダセキュアコンテナ（後述）と称する形態で、サービスプロバイダ３に供給する。

【００１８】

サービスプロバイダ３は、コンテンツプロバイダ２から供給されるUCPの利用

内容に対応して、１つまたは複数の価格情報（以下、PT(Price Tag)と記述する）を作成し、保持する。サービスプロバイダ２は、作成したPTを、コンテンツプロバイダ２から供給されたコンテンツ（コンテンツ鍵Ｋｃｏで暗号化されている）、コンテンツ鍵Ｋｃｏ（配送用鍵Ｋｄで暗号化されている）、およびUCPとともに、サービスプロバイダセキュアコンテナと称する形態で、専用のケーブルネットワーク、インターネット、または衛星通信などから構成されるネットワーク４を介して、ユーザホームネットワーク５に送信する。

【００１９】

ユーザホームネットワーク５は、供給されたUCPおよびPTに基づいて、使用許諾条件情報（以下、UCS(Usage Control Status)と称する）を作成し、作成したUCSに基づいてコンテンツを利用する処理を実行する。ユーザホームネットワーク５はまた、UCSを作成するタイミングで課金情報を作成し、例えば、配送用鍵Ｋｄの供給を受けるタイミングで、EMDサービスセンタ１に送信する。

【００２０】

図３は、EMDサービスセンタ１の機能的構成を示すブロック図である。サービスプロバイダ管理部１１は、サービスプロバイダ３に利益分配の情報を供給する。コンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に配送用鍵Ｋｄを送信したり、利益分配の情報を供給する。

【００２１】

著作権管理部１３は、ユーザホームネットワーク５のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC(Japanese Society for Rights of Authors,Composers and Publishers:日本音楽著作権協会)に送信する。

【００２２】

鍵サーバ１４は、配送用鍵Ｋｄを記憶しており、それを、コンテンツプロバイダ管理部１２を介してコンテンツプロバイダ２に供給したり、ユーザ管理部１８等を介してユーザホームネットワーク５に供給する。

【００２３】

ユーザホームネットワーク５の機器およびコンテンツプロバイダ２に供給される、EMDサービスセンタ１からの配送用鍵Ｋｄについて、図４乃至図７を参照して説明する。

【００２４】

図４は、コンテンツプロバイダ２がコンテンツの提供を開始し、ユーザホームネットワーク５を構成するレシーバ５１がコンテンツの利用を開始する、１９９８年１月における、EMDサービスセンタ１が有する配送用鍵Ｋｄ、コンテンツプロバイダ２が有する配送用鍵Ｋｄ、およびレシーバ５１が有する配送用鍵Ｋｄを示す図である。

【００２５】

図４の例において、配送用鍵Ｋｄは、暦の月の初日から月の末日まで、使用可能であり、たとえば、所定のビット数の乱数である”ａａａａａａａａ”の値を有するバージョン１である配送用鍵Ｋｄは、１９９８年１月１日から１９９８年１月３１日まで使用可能（すなわち、１９９８年１月１日から１９９８年１月３１日の期間にサービスプロバイダ３を介してユーザホームネットワーク５に配布されるコンテンツを暗号化するコンテンツ鍵Ｋｃｏは、バージョン１である配送用鍵Ｋｄで暗号化されている）であり、所定のビット数の乱数である”ｂｂｂｂｂｂｂｂ”の値を有するバージョン２である配送用鍵Ｋｄは、１９９８年２月１日から１９９８年２月２８日まで使用可能（すなわち、その期間にサービスプロバイダ３を介してユーザホームネットワーク５に配布されるコンテンツを暗号化するコンテンツ鍵Ｋｃｏは、バージョン２である配送用鍵Ｋｄで暗号化されている）である。同様に、バージョン３である配送用鍵Ｋｄは、１９９８年３月中に使用可能であり、バージョン４である配送用鍵Ｋｄは、１９９８年４月中に使用可能であり、バージョン５である配送用鍵Ｋｄは、１９９８年５月中に使用可能であり、バージョン６である配送用鍵Ｋｄは、１９９８年６月中に使用可能である。

【００２６】

コンテンツプロバイダ２がコンテンツの提供を開始するに先立ち、EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年１月から１９９８年６月

まで利用可能な、バージョン１乃至バージョン６の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、記憶する。６月分の配送用鍵Ｋｄを記憶するのは、コンテンツプロバイダ２が、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

【００２７】

また、レシーバ５１がコンテンツの利用を開始するに先立ち、EMDサービスセンタ１は、レシーバ５１に、１９９８年１月から１９９８年３月まで、利用可能なバージョン１乃至バージョン３である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、記憶する。３月分の配送用鍵Ｋｄを記憶するのは、レシーバ５１が、EMDサービスセンタ１に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、EMDサービスセンタ１への接続の頻度を低くし、ユーザホームネットワーク５の負荷を低減するためである。

【００２８】

１９９８年１月１日から１９９８年１月３１日の期間には、バージョン１である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００２９】

１９９８年２月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図５で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年２月から１９９８年７月まで利用可能な、バージョン２乃至バージョン７の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年２月から１９９８年４月まで、利用可能なバージョン２乃至バージョン４である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン

１である配送用鍵Ｋｄをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵Ｋｄを利用できるようにするためである。

【００３０】

１９９８年2月１日から１９９８年２月２８日の期間には、バージョン２である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００３１】

１９９８年３月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図６で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年３月から１９９８年８月まで利用可能な、バージョン３乃至バージョン８の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年３月から１９９８年５月まで、利用可能なバージョン３乃至バージョン５である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵Ｋｄおよびバージョン２である配送用鍵Ｋｄをそのまま記憶する。

【００３２】

１９９８年３月１日から１９９８年３月３１日の期間には、バージョン３である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００３３】

１９９８年４月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図７で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年４月から１９９８年９月まで利用可能な、バージョン４乃至バージョン９の６つの配送用鍵Ｋｄを送信し

、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年４月から１９９８年６月まで、利用可能なバージョン３乃至バージョン５である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵Ｋｄ、バージョン２である配送用鍵Ｋｄ、およびバージョン３である配送用鍵Ｋｄをそのまま記憶する。

【００３４】

１９９８年４月１日から１９９８年４月３０日の期間には、バージョン４である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００３５】

このように、あらかじめ先の月の配送用鍵Ｋｄを配布しておくことで、仮にユーザが１，２ヶ月まったくEMDサービスセンタ１にアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、EMDサービスセンタ１にアクセスして鍵を受信することができる。

【００３６】

図３に戻り、経歴データ管理部１５は、ユーザ管理部１８から出力される、課金情報、そのコンテンツに対応するPT、およびそのコンテンツに対応するUCPなどを記憶する。

【００３７】

利益分配部１６は、経歴データ管理部１５から供給された各種情報に基づき、EMDサービスセンタ１、コンテンツプロバイダ２、およびサービスプロバイダ３の利益をそれぞれ算出し、その結果をサービスプロバイダ管理部１１、コンテンツプロバイダ管理部１２、出納部２０、および著作権管理部１３に出力する。

【００３８】

相互認証部１７は、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の機器と相互認証を実行する。ユーザ管理部１８は

、所定の処理に対応して登録リスト（後述）を作成し、配送用鍵Ｋｄとともにユーザホームネットワーク５に送信する。

【００３９】

課金請求部１９は、経歴データ管理部１５から供給された、例えば、課金情報、UCP、およびPTに基づき、ユーザへの課金を算出し、その結果を、出納部２０に供給する。出納部２０は、ユーザ、コンテンツプロバイダ２、およびサービスプロバイダ３への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。出納部２０はまた、決算処理の結果をユーザ管理部１８に通知する。

【００４０】

監査部２１は、ユーザホームネットワーク５の機器から供給された課金情報、PT、およびUCPの正当性（すなわち、不正をしていないか）を監査する。なお、この場合、EMDサービスセンタ１は、コンテンツプロバイダ２からのUCPを、サービスプロバイダ３からのPTを、そしてユーザホームネットワーク５からのUCPとPTを、それぞれ受け取る。

【００４１】

図８は、コンテンツプロバイダ２の機能的構成を示すブロック図である。コンテンツサーバ３１は、ユーザに供給するコンテンツを記憶し、ウォータマーク付加部３２に供給する。ウォータマーク付加部３２は、コンテンツサーバ３１から供給されたコンテンツにウォータマーク（電子透かし）を付加し、圧縮部３３に供給する。

【００４２】

圧縮部３３は、ウォータマーク付加部３２から供給されたコンテンツを、ATRAC2(Adaptive Transform Acoustic Coding 2)（商標）等の方式で圧縮し、暗号化部３４に供給する。暗号化部３４は、圧縮部３３で圧縮されたコンテンツを、乱数発生部３５から供給された乱数を鍵（以下、この乱数をコンテンツ鍵Ｋｃｏと称する）として、DES(Data Encryption Standard)などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部３８に出力する。

【００４３】

乱数発生部３５は、コンテンツ鍵Ｋｃｏとなる所定のビット数の乱数を暗号化部３４および暗号化部３６に供給する。暗号化部３６は、コンテンツ鍵Ｋｃｏを EMDサービスセンタ１から供給された配送用鍵Ｋｄを使用して、DESなどの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部３８に出力する。

【００４４】

DESは、５６ビットの共通鍵を用い、平文の６４ビットを１ブロックとして処理する暗号方式である。DESの処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。DESのすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

【００４５】

まず、平文の６４ビットは、上位３２ビットのH_0、および下位３２ビットのL_0に分割される。鍵処理部から供給された４８ビットの拡大鍵K_1、および下位３２ビットのL_0を入力とし、下位３２ビットのL_0を攪拌したＦ関数の出力が算出される。Ｆ関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の２種類の基本変換から構成されている。次に、上位３２ビットのH_0と、Ｆ関数の出力が排他的論理和され、その結果はL_1とされる。L_0は、H_1とされる。

【００４６】

上位３２ビットのH_0および下位３２ビットのL_0を基に、以上の処理を１６回繰り返し、得られた上位３２ビットのH_{16}および下位３２ビットのL_{16}が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

【００４７】

ポリシー記憶部３７は、コンテンツに対応して設定されるUCPを記憶し、セキュアコンテナ作成部３８に出力する。図９は、コンテンツサーバ３１に保持されているコンテンツＡに対応して設定され、ポリシー記憶部３７に記憶されているUCPＡ，Ｂを表している。UCPは、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「利用条件」、「利用内容」の各項

目に対応する所定の情報が含まれる。「コンテンツのID」には、UCPが対応するコンテンツのIDが設定される。UCPA（図９（A））およびUCPB（図９（B））のそれぞれの「コンテンツのID」には、コンテンツAのIDが設定されている。

【００４８】

「コンテンツプロバイダのID」には、コンテンツの提供元のコンテンツプロバイダのIDが設定される。UCPAおよびUCPBのそれぞれの「コンテンツプロバイダのID」には、コンテンツプロバイダ２のIDが設定されている。「UCPのID」には、各UCPに割り当てられた所定のIDが設定され、UCPAの「UCPのID」には、UCPAのIDが、UCPBの「UCPのID」には、UCPBのIDが、それぞれ設定されている。「UCPの有効期限」には、UCPの有効期限を示す情報が設定され、UCPAの「UCPの有効期限」には、UCPAの有効期限が、UCPBの「UCPの有効期限」には、UCPBの有効期限が、それぞれ設定されている。

【００４９】

「利用条件」には、「ユーザ条件」および「機器条件」の各項目に対応する所定の情報が設定され、「ユーザ条件」には、このUCPを選択することができるユーザの条件が設定され、「機器条件」には、このUCPを選択することができる機器の条件が設定されている。

【００５０】

UCPAの場合、「利用条件１０」が設定され、「利用条件１０」の「ユーザ条件１０」には、所定の利用ポイントが２００ポイント以上が条件であることを示す情報（”２００ポイント以上”）が設定されている。また「利用条件１０」の「機器条件１０」には、条件がないことを示す情報（”条件なし”）が設定されている。すなわち、UCPAは、２００ポイント以上の利用ポイントを有するユーザのみが選択可能となる。

【００５１】

UCPBの場合、「利用条件２０」が設定され、「利用条件２０」の「ユーザ条件２０」には、所定の利用ポイントが２００ポイントより少ないことが条件であることを示す情報（”２００ポイントより少ない”）が設定されている。また「利用条件２０」の「機器条件２０」には、”条件なし”が設定されている。すな

わち、UCPＢは、２００ポイントより少ない利用ポイントを有するユーザのみが選択可能となる。

【００５２】

「利用内容」には、「ID」、「形式」、「パラメータ」、および「管理移動許可情報」の各項目に対応する所定の情報が含まれる。「ID」には、「利用内容」に設定される情報に割り当てられた所定のIDが設定される。「形式」には、再生や複製など、コンテンツの利用形式を示す情報が設定される。「パラメータ」には、「形式」に設定された利用形式に対応する所定の情報が設定される。

【００５３】

「管理移動許可情報」には、コンテンツの管理移動が可能か否か（許可されているか否かを示す情報（”可”または”不可”））が設定される。コンテンツの管理移動が行われると、図１０（Ａ）に示すように、管理移動元の機器にコンテンツが保持されつつ、管理移動先の機器にそのコンテンツが移動される。すなわち、管理移動元の機器と管理移動先の機器の両方において、コンテンツが利用される。この点で、図１０（Ｂ）に示すように、移動元の機器にコンテンツが保持されず、移動先の機器のみにコンテンツが保持され、移動先の機器においてのみコンテンツが利用される、通常の移動とは異なる。

【００５４】

また、コンテンツの管理移動が行われている間、管理移動元の機器は、図１０（Ａ）に示すように、他の機器にコンテンツを管理移動することができない（許可されない）。すなわち、管理移動元の機器と管理移動先の機器の２機においてのみコンテンツが保持される。この点で、図１１（Ａ）に示すように、オリジナルのコンテンツから、複数の複製（第１世代）を作成することができる、第１世代の複製とも異なる。また、管理移動元の機器からコンテンツを戻すことより、他の機器にコンテンツを管理移動することができるので、この点で、図１１（Ｂ）に示すように、１回だけの複製とも異なる。

【００５５】

図９（Ａ）に戻り、UCPＡには、４つの「利用内容１１」乃至「利用内容１４」が設けられており、「利用内容１１」において、その「ID１１」には、「利用

内容１１」に割り当てられた所定のIDが設定されている。「形式１１」には、コンテンツを買い取って再生する利用形式を示す情報（”買い取り再生”）が設定され、「パラメータ１１」には、”買い取り再生”に対応する所定の情報が設定されている。「管理移動許可情報１１」には、コンテンツの管理移動が許可されていることを示す情報（”可”）が設定されている。

【００５６】

「利用内容１２」において、その「ID１２」には、「利用内容１２」に割り当てられた所定のIDが設定されている。「形式１２」には、第１世代の複製を行う利用形式を示す情報（”第１世代複製”）が設定されている。第１世代複製は、図１１（Ａ）に示したように、オリジナルのコンテンツから、複数の第１世代の複製を作成することができる。ただし、第１世代の複製から第２世代の複製を作成することはできない（許可されない）。「パラメータ１２」には、”第１世代複製”に対応する所定の情報が設定されている。「管理移動許可情報１２」には、コンテンツの管理移動が許可されていないことを示す情報（”不可”）が設定されている。

【００５７】

「利用内容１３」において、その「ID１３」には、「利用内容１３」に割り当てられた所定のIDが設定されている。「形式１３」には、所定の期間（時間）に限って再生する利用形式を示す情報（”期間制限再生”）が設定され、「パラメータ１３」には、”期間制限再生”に対応して、その期間の開始時期（時刻）と終了時期（時刻）が設定されている。「管理移動許可情報１３」には、”不可”が設定されている。

【００５８】

「利用内容１４」において、その「ID１４」には、「利用内容１４」に割り当てられた所定のIDが設定されている。「形式１４」には、５回の複製を行う利用形式を示す情報（”Pay Per Copy５”）が設定されている。なお、この場合も、図１１の（Ｂ）に示すように、複製からの複製を作成することはできない（許可されない）。「パラメータ１４」には、複製が５回可能であることを示す情報（”複製５回”）が設定されている。「管理移動許可情報１４」には、”不可”が

設定されている。

【００５９】

図９（Ｂ）のUCPＢには、２つの「利用内容２１」、および「利用内容２２」が設けられている。「利用内容２１」において、その「ID２１」には、「利用内容２１」に割り当てられた所定のIDが設定されている。「形式２１」には、４回の再生を行う利用形式を示す情報（”Pay Per Play4”）が設定され、「パラメータ２１」には、再生が４回可能であることを示す情報”再生４回”が設定されている。「管理移動許可情報２１」には、”不可”が設定されている。

【００６０】

「利用内容２２」において、その「ID２２」には、「利用内容２２」に割り当てられた所定のIDが設定されている。「形式２２」には、”Pay Per Copy２”が設定され、「パラメータ２２」には、”複製２回”が設定されている。「管理移動許可情報２２」には、”不可”が設定されている。

【００６１】

ここで、UCPＡおよびUCPＢの内容を比較すると、２００ポイント以上の利用ポイントを有するユーザは、４通りの利用内容１１乃至利用内容１４から利用内容を選択することができるのに対して、２００ポイントより少ない利用ポイントを有するユーザは、２通りの利用内容２１，２２からしか利用内容を選択することができないものとされている。

【００６２】

ところで、図９は、UCPＡおよびUCPＢを模擬的に表しているが、例えば、UCPＡの「利用条件１０」およびUCPＢの「利用条件２０」には、実際は、図１２（Ａ）に示すサービスコード、および図１２（Ｂ）に示すコンディションコードの他、サービスコードに対応して数値や所定の種類を示すバリューコードがそれぞれ設定されている。

【００６３】

図１３（Ａ）は、UCPＡ（図９（Ａ））の「利用条件１０」の「ユーザ条件１０」および「機器条件１０」として設定されている各コードのコード値を表している。UCPＡの「利用条件１０」の「ユーザ条件１０」は、”２００ポイント以

上”とされているので、”利用ポイントに関し条件有り”を意味する８０ｘｘｈのサービスコード（図１２（Ａ））が、このとき数値２００を示す０００Ｃ８ｈのバリューコードが、そして”＞＝（以上）”を意味する０６ｈのコンディションコード（図１２（Ｂ））が、ユーザ条件として設定されている。

【００６４】

UCPAの「機器条件１０」は、”条件なし”とされているので、”条件なし”を意味する００００ｈのサービスコードが、このとき何ら意味を持たないＦＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコードが、機器条件として設定されている。

【００６５】

図１３（Ｂ）は、UCPBの「利用条件２０」の「ユーザ条件２０」および「機器条件２０」として設定されている各コードのコード値を表している。「ユーザ条件２０」は、”２００ポイントより少ない”とされているので、”利用ポイントに関し条件有り”を意味する８０ｘｘｈのサービスコードが、数値２００を示す０００Ｃ８ｈのバリューコードが、そして”＜（より小さい）”を意味する０３ｈのコンディションコードが、ユーザ条件として設定されている。

【００６６】

UCPBの「機器条件２０」は、UCPAの「機器条件１０」と同様に、”条件なし”とされ、同一のコード値が設定されているので、その説明は省略する。

【００６７】

図８に戻り、セキュアコンテナ作成部３８は、例えば、図１４に示すような、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、UCPA，Ｂ、および署名からなるコンテンツプロバイダセキュアコンテナを作成する。なお、署名は、送信したいデータ（この場合、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている））、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、およびUCPA，Ｂの全体にハッシュ関数を適用して得られたハッシュ値が、公開鍵暗号の秘密鍵（この場合、コンテンツプロバイダ２の秘密鍵Ｋｓｃｐ）で暗号化されたものである。

【００６８】

セキュアコンテナ作成部３８はまた、コンテンツプロバイダセキュアコンテナに、図１５に示すコンテンツプロバイダ２の証明書を付してサービスプロバイダ３に送信する。この証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ２に対し割り付けた証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、およびコンテンツプロバイダ２の名前、コンテンツプロバイダ２の公開鍵Ｋｐｃｐ、並びにその署名（認証局の秘密鍵Ｋｓｃａで暗号化されている）から構成されている。

【００６９】

署名は、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

【００７０】

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

【００７１】

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD4, MD5, SHA-1などが用いられる。

【００７２】

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を

使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

【００７３】

公開鍵暗号の中で代表的なRSA（Rivest-Shamir-Adleman）暗号を、簡単に説明する。まず、２つの十分に大きな素数であるpおよびqを求め、さらにpとqの積であるｎを求める。(p-1)と(q-1)の最小公倍数Lを算出し、更に、３以上L未満で、かつ、Ｌと互いに素な数eを求める（すなわち、eとLを共通に割り切れる数は、１のみである）。

【００７４】

次に、Lを法とする乗算に関するeの乗法逆元dを求める。すなわち、d，e、およびLの間には、ed=1 mod Lが成立し、dはユークリッドの互除法で算出できる。このとき、nとeが公開鍵とされ、p,q,およびdが、秘密鍵とされる。

【００７５】

暗号文Cは、平文Mから、式（１）の処理で算出される。

【００７６】

C=M^e mod n　　(1)

暗号文Cは、式（２）の処理で平文Mに、復号される。

【００７７】

M=C^d mod n　　（２）

証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式（３）が成立するからである。

【００７８】

M=C^d=(M^e)^d=M^(ed)=M mod n　　（３）

秘密鍵pとqを知っているならば、公開鍵eから秘密鍵dは算出できるが、公開鍵nの素因数分解が計算量的に困難な程度に公開鍵nの桁数を大きくすれば、公開鍵nを知るだけでは、公開鍵eから秘密鍵dは計算できず、復号できない。以上のように、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とす

ることができる。

【００７９】

また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線y^2=x^3+ax+b上の、ある点をBとする。楕円曲線上の点の加算を定義し、nBは、Bをn回加算した結果を表す。同様に、減算も定義する。BとnBからnを算出することは、困難であることが証明されている。BとnBを公開鍵とし、nを秘密鍵とする。乱数rを用いて、暗号文C1およびC2は、平文Mから、公開鍵で式（４）および式（５）の処理で算出される。

【００８０】

C1=M+rnB　（４）

C2=rB　（５）

暗号文C1およびC2は、式（６）の処理で平文Mに、復号される。

【００８１】

M=C1-nC2　（６）

復号できるのは、秘密鍵nを有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【００８２】

図８に、再び戻り、コンテンツプロバイダ２の相互認証部３９は、EMDサービスセンタ１から配送用鍵Ｋｄの供給を受けるのに先立ち、EMDサービスセンタ１と相互認証する。また相互認証部３９は、サービスプロバイダ３へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ３と相互認証することも可能であるが、この例の場合、コンテンツプロバイダセキュアコンテナには、秘密しなければならない情報が含まれていないので、この相互認証は必ずしも必要とされるわけではない。

【００８３】

次に、図１６のブロック図を参照して、サービスプロバイダ３の機能的構成を説明する。コンテンツサーバ４１は、コンテンツプロバイダ２から供給されたコンテンツプロバイダセキュアコンテナに含まれる、コンテンツ（コンテンツ鍵K

ｃｏで暗号化されている）、コンテンツ鍵Ｋｃｏ（配送用鍵Ｋｄで暗号化されている）、UCP、およびコンテンツプロバイダ２の署名を記憶し、セキュアコンテナ作成部４４に供給する。

【００８４】

値付け部４２は、コンテンツプロバイダ２から供給されたコンテンツプロバイダセキュアコンテナに含まれる署名に基づいて、コンテンツプロバイダセキュアコンテナの正当性を検証するが、この場合、コンテンツプロバイダ２の証明書が検証され、正当であるとき、コンテンツプロバイダ２の公開鍵が取得される。そしてこの取得された公開鍵に基づいて、コンテンツプロバイダセキュアコンテナの正当性が検証される。

【００８５】

コンテンツプロバイダセキュアコンテナの正当性を確認すると、値付け部４２は、コンテンツプロバイダセキュアコンテナに含まれるUCPに対応する、PTを作成し、セキュアコンテナ作成部４４に供給する。図１７は、図９（Ａ）のUCPＡに対応して作成された、２つのPTＡ－１（図１７（Ａ））およびPTＡ－２（図１７（Ｂ））を表している。PTには、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「価格条件」、および「価格内容」の各項目に対応する所定の情報が含まれる。

【００８６】

PTの、「コンテンツのID」、「コンテンツプロバイダのID」、および「UCPのID」の各項目には、UCPの、これらに対応する項目の情報が、それぞれ設定される。すなわち、PTＡ－１およびPTＡ－２のそれぞれの「コンテンツのID」には、コンテンツＡのIDが、それぞれの「コンテンツプロバイダのID」には、コンテンツプロバイダ２のIDが、そしてそれぞれの「UCPのID」には、UCPＡのIDが設定されている。

【００８７】

「サービスプロバイダのID」には、PTの提供元のサービスプロバイダ２のIDが設定される。PTＡ－１およびPTＡ－２のそれぞれの「サービスプロバイダのID」

には、サービスプロバイダ３のIDが設定されている。「PTのID」には、各PTに割り当てられた所定のIDが設定される。PTA－１の「PTのID」には、PTA－１のIDが、PTA－２の「PTのID」には、PTA－２のIDがそれぞれ設定されている。「PTの有効期限」には、PTの有効期限を示す情報が設定される。PTA－１の「PTの有効期限」には、PTA－１の有効期限が、PTA－２の「PTの有効期限」には、PTA－２の有効期限が設定されている。

【００８８】

「価格条件」には、UCPの「利用条件」と同様に、「ユーザ条件」および「機器条件」の各項目に対応する所定の情報が設定されている。「価格条件」の「ユーザ条件」には、このPTを選択することができるユーザの条件を示す情報が設定され、その「機器条件」には、このPTを選択することができる機器の条件を示す情報が設定される。

【００８９】

PTA－１の場合、「価格条件１０」が設定され、「価格条件１０」の「ユーザ条件１０」には、ユーザが男性であるを示す情報（”男性”）が設定され、その「機器条件１０」には、”条件なし”が設定されている。すなわち、PTA－１は、男性のユーザのみが選択可能となる。

【００９０】

PTA－１の「価格条件１０」の「ユーザ条件１０」および「機器条件１０」も、実際は、図１８（A）に示すように、各種コードのコード値が設定されている。「価格条件１０」の「ユーザ条件１０」には、”性別条件有り”を意味する０１ｘｘｈのサービスコード（図１２（A））が、このとき男性を意味する００００００ｈのバリューコードが、そして”＝”を意味する０１ｈのコンディションコード（図１２（B））が設定されている。「機器条件１０」には、”条件なし”を意味する００００ｈのサービスコードが、この場合何ら意味を持たないＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコードが設定されている。

【００９１】

PTA－２の場合、「価格条件２０」が設定され、「価格条件２０」の「ユーザ

条件２０」には、ユーザが女性であることを示す情報（”女性”）が設定され、その「機器条件２０」には、”条件なし”が設定されている。すなわち、PTA－２は、女性のユーザのみが選択可能となる。

【００９２】

PTA－２の「価格条件２０」の「ユーザ条件２０」および「機器条件２０」も、実際は、図１８（B）に示すように、各コードのコード値が設定されている。「価格条件２０」の「ユーザ条件２０」には、”性別条件有り”を意味する０１ｘｘｈのサービスコード（図１２（A））が、この場合女性を示す０００００１ｈのバリューコードが、そして”＝”を意味する０１ｈのコンディションコード（図１２（B））が設定されている。その「機器条件２０」には、”条件なし”を意味する０００００ｈのサービスコードが、この場合何ら意味を持たないＦＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコードが設定されている。

【００９３】

図１７に戻り、PTの「価格内容」には、対応するUCPの「利用内容」の「形式」に設定されている利用形式の利用料金が示されている。すなわち、PTA－１の「価格内容１１」に設定された”２０００円”およびPTA－２の「価格内容２１」に設定された”１０００円”は、UCPA（図９（A））の「利用内容１１」の「形式１１」が”買い取り再生”とされているので、コンテンツＡの買い取り価格（料金）を示している。

【００９４】

PTA－１の「価格内容１２」の”６００円”およびPTA－２の「価格内容２２」の”３００円”は、UCPAの「利用内容１２」の「形式１２」より、第１世代複製の利用形式でコンテンツＡを利用する場合の料金を示している。PTA－１の「価格内容１３」の”１００円”およびPTA－２の「価格内容２３」の”５０円”は、UCPAの「利用内容１３」の「形式１３」より、期間制限再生の利用形式でコンテンツＡを利用する場合の料金を示している。PTA－１の「価格内容１４」の”３００円”およびPTA－２の「価格内容２４」の”１５０円”は、UCPAの「利用内容１４」の「形式１４」より、５回の複製を行う利用形式でコンテン

ツＡを利用する場合の料金を示している。

【００９５】

なお、この例の場合、PTA－１（男性ユーザに適用される）の価格内容と、PTA－２（女性ユーザに適用される）の価格内容を比較すると、PTA－１の価格内容に示される価格が、PTA－２の価格内容に示される価格の２倍に設定されている。例えば、UCPAの「利用内容１１」に対応するPTA－１の「価格内容１１」が”２０００円”とされているのに対し、同様にUCPAの「利用内容１１」に対応するPTA－２の「価格内容２１」は”１０００円”とされている。同様に、PTA－１の「価格内容１２」乃至「価格内容１４」に設定されている価格は、PTA－２の「価格内容２２」乃至「価格内容２４」に設定されている価格に２倍とされている。すなわち、この例の場合、コンテンツＡは、女性のユーザがより低価格で利用できるコンテンツとされている。

【００９６】

図１９は、図９（Ｂ）のUCPBに対応して作成された、２つのPTB－１およびPTB－２を表している。図１９（Ａ）のPTB－１には、コンテンツＡのID、コンテンツプロバイダ２のID、UCPBのID、UCPBの有効期限、サービスプロバイダ３のID、PTB－１のID、PTB－１の有効期限、価格条件３０、２通りの価格内容３１，３２などが含まれている。

【００９７】

PTB－１の「価格条件３０」の「ユーザ条件３０」には”条件なし”が設定され、「機器条件３０」には、機器が従機器であることを条件とする情報（”従機器”）が設定されている。すなわち、PTB－１は、コンテンツＡが従機器において利用される場合にのみ選択可能となる。なお、従機器とは、自分自身が、所定のコンテンツを購入するための処理や、課金を決済する処理などを行うことができない機器を意味する。

【００９８】

PTB－１の「価格条件３０」の「ユーザ条件３０」および「機器条件３０」にも、実際は、図２０（Ａ）に示すように、各コードのコード値が設定されている。「ユーザ条件３０」には、”条件なし”を意味する０００００ｈのサービスコー

ド（図１２（Ａ））が、この場合何ら意味を持たないＦＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコード（図１２（Ｂ））が設定されている。「機器条件３０」は、”従機器”とされているので、”機器に関し条件有り”を意味する００ｘｘｈのサービスコードが、このとき”数値１００”を示す０００００６４ｈのバリューコードが、そして”＜（小さい）”を意味する０３ｈのコンディションコードが設定されている。この例の場合、従機器には、１００番より小さい機器番号が設定されているので、このようなコード値が設定される。

【００９９】

PTB－１の「価格内容３１」の”１００円”は、UCPB（図９（Ｂ））の「利用内容２１」の「形式２１」が”Pay Per Play４”とされているので、４回の再生を行う場合の料金を示し、「価格内容３２」の”３００円”は、UCPBの「利用内容２２」の「形式２２」が”Pay Per Copy２”とされているので、２回の複製を行う場合の料金を示している。

【０１００】

UCPBに対応して作成された、もう一方のPTB－２には、図１９（Ｂ）に示すように、コンテンツＡのID、コンテンツプロバイダ２のID、UCPBのID、UCPB、サービスプロバイダ３のID、PTB－２のID、PTB－２の有効期限、価格条件４０、および２通りの価格内容４１，４２などが含まれている。

【０１０１】

PTB－２の「価格条件４０」の「ユーザ条件４０」には”条件なし”が設定され、その「機器条件４０」には、機器が主機器であることを条件とする情報（”主機器”）が設定されている。すなわち、PTB－２は、主機器においてコンテンツが利用される場合にのみ選択可能となる。なお、主機器とは、自分自身が、所定のコンテンツを購入するための処理や、課金を決済する処理などを行うことができる機器を意味する。

【０１０２】

PTB－２の「価格条件４０」の「ユーザ条件４０」および「機器条件４０」にも、実際は、図２０（Ｂ）に示すように、各コードのコード値が設定されている

。「価格条件４０」の「ユーザ条件４０」には、”条件なし”を意味する００００ｈのサービスコード（図１２（Ａ））が、この場合何ら意味を持たないＦＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコード（１５（Ｂ））が設定されている。「機器条件４０」には、”機器に関し条件有り”を意味する００ｘｘｈのサービスコードが、このとき”数値１００”を示す０００００６４ｈのバリューコードが、そして”＝＞（以上）”を意味する０６ｈのコンディションコードが設定されている。この例の場合、主機器には、１００番以上の機器番号が設定されているので、このようなコード値が設定される。

【０１０３】

PTB－２の「価格内容４１」および「価格内容４２」のそれぞれに示される価格は、UCPBの「利用内容２１」の「形式２１」および「利用内容２２」の「形式２２」のそれぞれに示される利用形式でコンテンツＡを利用する場合の料金を示している。

【０１０４】

ここで、PTB－１（従機器に適用される）の価格内容とPTB－２（主機器に適用される）の価格内容を比較すると、PTB－１の価格内容は、PTB－２の価格内容の２倍に設定されている。例えば、PTB－１の「価格内容３１」が”１００円”とされているのに対し、PTB－２の「価格内容４１」は５０円とされており、「価格内容３２」が”３００円”とされているのに対して、「価格内容４２」は”１５０円”とされている。

【０１０５】

図１６に戻り、ポリシー記憶部４３は、コンテンツプロバイダ２から供給された、コンテンツのUCPを記憶し、セキュアコンテナ作成部４４に供給する。

【０１０６】

セキュアコンテナ作成部４４は、例えば、図２１に示すような、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、UCPA，Ｂ、コンテンツプロバイダ２の署名、PTＡ－１，Ａ－２，Ｂ－１，Ｂ－２、およびサービスプロバイダ３の署名からなる

サービスプロバイダセキュアコンテナを作成する。

【０１０７】

セキュアコンテナ作成部４４はまた、作成したサービスプロバイダセキュアコンテナを、図２２に示すような、証明書のバージョン番号、認証局がサービスプロバイダ３に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ３の名前、サービスプロバイダ３の公開鍵Ｋｐｓｐ、並びに署名より構成されるサービスプロバイダの証明書を付して、ユーザホームネットワーク５に供給する。

【０１０８】

図１６に、再び戻り、相互認証部４５は、コンテンツプロバイダ２からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ２と相互認証する。相互認証部４５また、ユーザホームネットワーク５へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク５と相互認証するが、このサービスプロバイダ３とユーザホームネットワーク５との相互認証は、例えば、ネットワーク４が衛星通信である場合、実行されない。なお、この例の場合、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナには、特に、秘密情報が含まれていないので、サービスプロバイダ３は、コンテンツプロバイダ２およびユーザホームネットワーク５と相互認証を行わなくてもよい。

【０１０９】

図２３は、ユーザホームネットワーク５を構成するレシーバ５１の構成例を表している。レシーバ５１は、通信部６１、SAM６２、外部記憶部６３、伸張部６４、通信部６５、インタフェース６６、表示制御部６７、および入力制御部６８より構成される、HDD５２に接続される据え置き型の機器である。

【０１１０】

レシーバ５１の通信部６１は、ネットワーク４を介してサービスプロバイダ３、またはEMDサービスセンタ１と通信し、所定の情報を受信し、または送信する。

【０１１１】

SAM６２は、相互認証モジュール７１、課金処理モジュール７２、記憶モジュール７３、復号／暗号化モジュール７４、およびデータ検査モジュール７５からなるが、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパー性）を有している。

【０１１２】

SAM６２の相互認証モジュール７１は、記憶モジュール７３に記憶されている、図２４に示すSAM６２の証明書を、相互認証相手に送信し、相互認証を実行し、これにより、認証相手と共有することとなった一時鍵Ｋｔｅｍｐ（セッション鍵）を復号／暗号化モジュール７４に供給する。SAMの証明書には、コンテンツプロバイダ２の証明書（図１５）およびサービスプロバイダ３の証明書（図２２）に含まれている情報に対応する情報が含まれているので、その説明は省略する。

【０１１３】

課金処理モジュール７２は、選択されたUCPの利用内容に基づいて、UCSおよび課金情報を作成する。図２５は、図９（Ａ）に示したUCPＡの利用内容１１と、図１７（Ａ）に示したPTＡ－１の価格内容１１に基づいて作成されたUCSＡを表している。UCSには、図２５に示されるように、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、「利用内容」、および「利用履歴」の各項目に対応する所定の情報が設定される。

【０１１４】

UCSの、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、および「PTの有効期限」の各項目には、PTの、それらに対応する項目の情報が設定される。すなわち、図２５のUCSＡの、「コンテンツのID」には、コンテンツＡのIDが、「コンテンツプロバイダのID」には、コンテンツプロバイダ２のIDが、「UCPのID

」には、UCPＡのIDが、「UCPの有効期限」には、UCPＡの有効期限が、「サービスプロバイダのID」には、サービスプロバイダ３のIDが、「PTのID」には、PTＡ－１のIDが、そして「PTの有効期限」には、PTＡ－１の有効期限が、それぞれ設定されている。

【０１１５】

「UCSのID」には、UCSに割り当てられた所定のIDが設定され、UCSAの「UCSのID」には、UCSＡのIDが設定されている。「SAMのID」には、機器のSAMのIDが設定され、UCSAの「SAMのID」には、レシーバ５１のSAM６２のIDが設定されている。「ユーザのID」には、コンテンツを利用するユーザのIDが設定され、UCSＡの「ユーザのID」には、レシーバ５１のユーザのIDが設定されている。

【０１１６】

「利用内容」は、「ID」、「形式」、「パラメータ」、および「管理移動状態情報」の各項目からなり、そのうち「ID」、「形式」、および「パラメータ」の項目には、選択されたUCPの「利用内容」の、それらに対応する項目の情報が設定される。すなわち、UCSＡの「ID」には、UCPＡの「利用内容１１」の「ID１１」に設定されている情報（利用内容１１のID）が、「形式」には、「利用内容１１」の「形式１１」に設定されている”買い取り再生”が、「パラメータ」には、「利用内容１１」の「パラメータ１１」に設定されている情報（”買い取り再生”に対応する情報）が設定されている。

【０１１７】

「利用内容」の「管理移動状態情報」には、選択されたUCPの「管理移動許可情報」に”可”が設定されている場合（管理移動が行える場合）、管理移動元の機器（コンテンツを購入した機器）と管理移動先の機器のそれぞれのIDが設定されるようになされている。なお、コンテンツの管理移動が行われていない状態においては、管理移動元の機器のIDが、管理移動先の機器のIDとしても設定される。一方、UCPの「管理移動許可情報」に、”不可”が設定されている場合、「管理移動状態情報」には”不可”が設定される。すなわち、この場合、コンテンツの管理移動は行われない（許可されない）。UCSＡの「管理移動状態情報」には、UCPＡの「利用内容１１」の「管理移動許可情報１１」に”可”が設定されて

おり、また、このとき、コンテンツＡは管理移動されていないので、SAM６２のIDが、管理移動元の機器のIDおよび管理移動先の機器のIDとして設定されている。

【０１１８】

「利用履歴」には、同一のコンテンツに対する利用形式の履歴が設定される。UCSAの「利用履歴」には、”買い取り再生”を示す情報のみが記憶されているが、例えば、レシーバ５１において、コンテンツＡが以前に利用されていた場合、そのときの利用形式も記憶される。

【０１１９】

なお、上述したUCSにおいては、「UCPの有効期限」および「PTの有効期限」が設けられているがそれらをUCSに設定しないようにすることもできる。また、上述したUCSにおいて、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

【０１２０】

作成されたUCSは、レシーバ５１の復号／暗号化モジュール７４の復号化ユニット９１から供給されるコンテンツ鍵Ｋｃｏ（保存用鍵Ｋｓａｖｅで暗号化されている）とともに、外部記憶部６３に送信され、その利用情報記憶部６３Ａに記憶される。外部記憶部６３の利用情報記憶部６３Ａは、図２６に示すように、Ｍ個のブロックＢＰ－１乃至ＢＰ－Ｍに分割され（例えば、１メガバイト毎に分割され）、各ブロックＢＰが、Ｎ個の利用情報用メモリ領域ＲＰ－１乃至ＲＰ－Ｎに分割されている。SAM６２から供給されるコンテンツ鍵Ｋｃｏ（保存用鍵Ｋｓａｖｅで暗号化されている）およびUCSは、利用情報用記憶部６３Ａの所定のブロックＢＰの利用情報用メモリ領域ＲＰに、対応して記憶される。

【０１２１】

図２６の例では、ブロックＢＰ－１の利用情報用メモリ領域ＲＰ－３に、図２５に示したUCSAとコンテンツ鍵ＫｃｏＡ（保存用鍵Ｋｓａｖｅで暗号化されてい

る）が対応して記憶されている。ブロックＢＰ－１の利用情報用メモリ領域ＲＰ－１，ＲＰ－２には、他のコンテンツ鍵Ｋｃｏ１，Ｋｃｏ２（それぞれ保存用鍵Ｋｓａｖｅで暗号化されている）およびUCS１，２がそれぞれ記憶されている。ブロックＢＰ－１の利用情報用メモリ領域ＲＰ－４（図示せず）乃至ＲＰ－Ｎ、およびブロックＢＰ－２（図示せず）乃至ＢＰ－Ｍには、この場合、コンテンツ鍵ＫｃｏおよびUCSは記憶されておらず、空いていることを示す所定の初期情報が記憶されている。なお、利用情報用メモリ領域ＲＰに記憶されるコンテンツ鍵Ｋｃｏ（保存用鍵Ｋｓａｖｅで暗号化されている）およびUCSを、個々に区別する必要がない場合、まとめて、利用情報と称する。

【０１２２】

図２７は、図２５に示したUCSＡと同時に作成された課金情報Ａを表している。課金情報は、図２７に示されるように、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、「利用内容」、および「課金履歴」の各項目に対応する所定の情報が設定される。

【０１２３】

課金情報の、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、および「利用内容」には、UCSの、それらに対応する項目の情報が、それぞれ設定される。すなわち、図２７の課金情報Ａの、「コンテンツのID」には、コンテンツＡのIDが、「コンテンツプロバイダのID」には、コンテンツプロバイダ２のIDが、「UCPのID」には、UCPＡのIDが、「UCPの有効期限」には、UCPＡの有効期限が、「サービスプロバイダのID」には、サービスプロバイダ３のIDが、「PTのID」には、PTＡ－１のIDが、「PTの有効期限」には、PTＡ－１の有効期限が、「UCSのID」には、UCSＡのIDが、「SAMのID」には、SAM６２のIDが、「ユーザのID」には、ユーザＦのIDが、そして「利用内容」には、UCSＡの「利用内容１１」の内容が、それぞれ設定されている。

【０１２４】

課金情報の「課金履歴」には、機器において計上された課金の合計額を示す情報が設定される。課金情報Ａの「課金履歴」には、レシーバ５１において計上された課金の合計額が設定されている。

【０１２５】

なお、上述した課金情報においては、「UCPの有効期限」および「PTの有効期限」が設けられているが、それらを課金情報に設定しないようにすることもできる。また、上述した課金情報においては、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

【０１２６】

図２３に戻り、記憶モジュール７３には、図２８に示すように、SAM６２の公開鍵Ｋｐｕ、SAM６２の秘密鍵Ｋｓｕ、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃ、認証局の公開鍵Ｋｐｃａ、保存用鍵Ｋｓａｖｅ、３月分の配送用鍵Ｋｄなどの各種鍵、SAM６２の証明書、課金情報、基準情報５１、およびＭ個の検査値HP－１乃至HP－Ｍなどが記憶されている。

【０１２７】

記憶モジュール７３に記憶される検査値HP－１は、外部記憶部６３の利用情報記憶部６３ＡのブロックＢＰ－１に記憶されているデータの全体にハッシュ関数が適用されて算出されたハッシュ値である。検査値HP－２乃至HP－Ｍも、検査値HP－１と同様に、外部記憶部６３の、対応するブロックＢＰ－２乃至ＢＰ－Ｍのそれぞれに記憶されているデータのハッシュ値である。

【０１２８】

図２９は、記憶モジュール７３に記憶されている基準情報５１を表している。基準情報には、「SAMのID」、「機器番号」、「決済ID」、「課金の上限額」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」の各項

目に設定される所定情報などが含まれている。

【０１２９】

基準情報５１には、SAM６２のID、SAM６２の機器番号（１００番）、ユーザの決済ID、ユーザの決済ユーザ情報（ユーザの一般情報（氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別）、ユーザのID、およびユーザのパスワード）、および所定の利用ポイント情報が設定されている。

【０１３０】

「課金の上限額」には、機器がEMDシステムに正式登録されている状態と仮登録されている状態で、それぞれ異なる課金の上限額が設定される。基準情報５１の「課金の上限額」には、レシーバ５１が正式登録されているので、正式登録されている状態における課金の上限額を示す情報（”正式登録時の上限額”）が設定されている。

【０１３１】

図２３に戻り、SAM６２の復号／暗号化モジュール７４は、復号ユニット９１、乱数発生ユニット９２、および暗号化ユニット９３から構成される。復号ユニット９１は、暗号化されたコンテンツ鍵Ｋｃｏを配送用鍵Ｋｄで復号し、暗号化ユニット９３に出力する。乱数発生ユニット９２は、必要に応じて（例えば、相互認証時に）、所定の桁数の乱数を発生し、必要に応じて一時鍵Ｋｔｅｍｐを生成し、暗号化ユニット９３に出力する。

【０１３２】

暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを、再度、記憶モジュール７３に保持されている保存用鍵Ｋｓａｖｅで暗号化する。暗号化されたコンテンツ鍵Ｋｃｏは、外部記憶部６３に供給される。暗号化ユニット９３は、コンテンツ鍵Ｋｃｏを伸張部６４に送信するとき、コンテンツ鍵Ｋｃｏを乱数発生ユニット９２で生成した一時鍵Ｋｔｅｍｐで暗号化する。

【０１３３】

データ検査モジュール７５は、記憶モジュール７３に記憶されている検査値HPと、外部記憶部６３の利用情報記憶部６３Ａの、対応するブロックBPのデータのハッシュ値を比較し、ブロックBPのデータが改竄されていないか否かを検査

する。

伸張部６４は、相互認証モジュール１０１、復号モジュール１０２、復号モジュール１０３、伸張モジュール１０４、およびウォータマーク付加モジュール１０５から構成される。相互認証モジュール１０１は、SAM６２と相互認証し、一時鍵Ｋｔｅｍｐを復号モジュール１０２に出力する。復号モジュール１０２は、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号し、復号モジュール１０３に出力する。復号モジュール１０３は、HDD５２に記録されたコンテンツをコンテンツ鍵Ｋｃｏで復号し、伸張モジュール１０４に出力する。伸張モジュール１０４は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォータマーク付加モジュール１０５に出力する。ウォータマーク付加モジュール１０５は、コンテンツにレシーバ５１を特定するための情報（例えば、SAM６２のID）のウォータマーク（電子透かし）を挿入し、図示せぬスピーカに出力し、音楽を再生する。

【０１３４】

通信部６５は、ユーザホームネットワーク５のレシーバ２０１との通信処理を行う。インターフェース６６は、SAM６２および伸張部６４からの信号を所定の形式に変更し、HDD５２に出力し、また、HDD５２からの信号を所定の形式に変更し、SAM６２および伸張部６４に出力する。

【０１３５】

表示制御部６７は、表示部（図示せず）への出力を制御する。入力制御部６８は、各種ボタンなどから構成される操作部（図示せず）からの入力を制御する。

【０１３６】

HDD５２は、サービスプロバイダ３から供給されたコンテンツなどを記憶する他、図３０に示すような登録リストを記憶している。この登録リストは、表形式に情報が記憶されているリスト部、および登録リストを保持する機器についての所定の情報が記憶されている対象SAM情報部より構成されている。

【０１３７】

対象SAM情報部には、この登録リストを保有する機器のSAMID、この例の場合、レシーバ５１のSAM６２のIDが（「対象SAMID」の欄に）記憶されている。対象SA

M情報部にはまた、この登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ５１には、レシーバ２０１の１機の機器が接続されているので、自分自身を含む合計値２が（「接続されている機器数」の欄に）記憶されている。

【０１３８】

リスト部は、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、「状態フラグ」、「公開鍵」、および「署名」の９個の項目から構成され、この例の場合、レシーバ５１の登録条件、レシーバ２０１の登録条件として、それぞれの項目に所定の情報が記憶されている。

【０１３９】

「SAMID」には、機器のSAMのIDが記憶される。この例の場合、レシーバ５１のSAM６２のID、およびレシーバ２０１のSAM２１２のIDが記憶されている。「ユーザID」には、対応する機器のユーザのユーザIDが記憶される。

【０１４０】

「購入処理」には、機器が、コンテンツを購入するための処理を行うことができるか否かを示す情報（”可”または”不可”）が記憶される。この例の場合、レシーバ５１およびレシーバ２０１は、コンテンツを購入するための処理を行うことができるようになされているので、それぞれに対応する「購入処理」には、”可”が記憶されている。

【０１４１】

「課金処理」には、機器が、EMDサービスセンタ１との間で、課金処理を行うことができるか否かを示す情報（”可”または”不可”）が記憶される。この例の場合、レシーバ５１のみが、課金処理を行うことができ、レシーバ２０１はその処理を行うことができないようになされているので、レシーバ５１に対応する「課金処理」には、”可”が記憶され、レシーバ２０１に対応する「課金処理」には、”不可”が記憶されている。

【０１４２】

「課金機器」には、機器において計上された課金を決済する処理を行う機器の

SAMのIDが記憶される。この例の場合、レシーバ５１（SAM６２）は、自分自身の課金を自分自身で決済することができるので、その対応する「課金機器」には、レシーバ５１のSAM６２のIDが記憶されている。レシーバ５１はまた、自分自身の課金を決済することができないレシーバ２０１に代わり、その課金を決済するようになされているので、レシーバ２０１に対応する「課金機器」には、レシーバ５１のSAM６２のIDが記憶されている。

【０１４３】

「コンテンツ供給機器」には、機器が、コンテンツの供給をサービスプロバイダ３からではなく、接続される他の機器から受ける場合、コンテンツを供給することができる機器のSAMのIDが記憶される。この例の場合、レシーバ５１およびレシーバ２０１は、コンテンツの供給をサービスプロバイダ３から受けるので、それぞれに対応する「コンテンツ供給機器」には、コンテンツを供給する機器が存在しない旨を示す情報（”なし”）が記憶されている。

【０１４４】

「状態フラグ」には、機器の動作制限条件が記憶される。何ら制限されていない場合は、その旨を示す情報（”制限なし”）、一定の制限が課せられている場合は、その旨を示す情報（”制限あり”）、また動作が停止される場合には、その旨を示す情報（”停止”）が記憶される。例えば、課金処理が成功しなかった場合、その機器に対応する「状態フラグ」には、”制限あり”が設定される（詳細は後述する）。この例の場合、「状態フラグ」に”制限あり”が設定された機器においては、すでに購入されたコンテンツの再生（解読）処理は実行されるが、新たなコンテンツを購入するための処理は実行されなくなる。すなわち、一定の制限が機器に課せられる。また、コンテンツの不正複製などの違反行為が発覚した場合、「状態フラグ」には、”停止”が設定され、機器の動作が停止される。これにより、その機器はEMDシステムからのサービスを、一切受けることができなくなる。

【０１４５】

この例の場合、レシーバ５１およびレシーバ２０１に対しては、何ら制限が課せられていないものとし、それぞれに対応する「状態フラグ」には、”なし”が

設定されている。なお、「状態フラグ」に設定される、”制限あり”および”停止”など、動作を制限するための情報を、個々に区別する必要がない場合、まとめて、動作制限情報と称する。

【０１４６】

「登録条件署名」には、各登録条件として、それぞれ、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、および「状態フラグ」に記憶されている情報に対するEMDサービスセンタ１による署名が記憶されている。「登録リスト署名」には、登録リストに設定されているデータの全体に対する署名が記憶されている。

【０１４７】

図３１は、レシーバ２０１の構成例を表している。レシーバ２０１の通信部２１１乃至入力制御部２１８は、レシーバ５１の通信部６１乃至入力制御部６８と同様の機能を有しているので、その詳細な説明は適宜省略する。

【０１４８】

HDD２０２には、購入したコンテンツの他、図３２に示すような、レシーバ２０１の登録リストが記憶されている。この登録リストの対象SAM情報部には、レシーバ２０１のSAM２１０のID、その登録リストの有効期限、バージョン番号、接続されている機器の数（この例では、レシーバ２０１には、レシーバ５１の１機が接続され、自分自身を含めた合計数２）が記憶されている。リスト部には、図３０のレシーバ５１の登録リストのリスト部と同様の情報が記憶されている。

【０１４９】

次に、EMDシステムの処理について、図３３のフローチャートを参照して説明するが、ここでは、コンテンツプロバイダ２に保持されているコンテンツＡが、サービスプロバイダ３を介して、ユーザホームネットワーク５のレシーバ５１に供給され、利用される場合を例として説明する。

【０１５０】

ステップＳ１１において、配送用鍵Ｋｄが、EMDサービスセンタ１からコンテンツプロバイダ２に供給される処理が行われる。この処理の詳細は、図３４のフローチャートに示されている。すなわち、ステップＳ３１において、EMDサービ

スセンタ１の相互認証部１７（図３）は、コンテンツプロバイダ２の相互認証部３９（図８）と相互認証し、コンテンツプロバイダ２が、正当なプロバイダであることが確認した後、EMDサービスセンタ１のコンテンツプロバイダ管理部１２は、鍵サーバ１４から供給された配送用鍵Ｋｄをコンテンツプロバイダ２に送信する。なお、相互認証処理の詳細は、図３５乃至図３７を参照して後述する。

【０１５１】

次に、ステップＳ３２において、コンテンツプロバイダ２の暗号化部３６は、EMDサービスセンタ１から送信された配送用鍵Ｋｄを受信し、ステップＳ３３において、記憶する。

【０１５２】

このように、コンテンツプロバイダ２の暗号化部３６が、配送用鍵Ｋｄを記憶したとき、処理は終了し、図３３のステップＳ１２に進む。ここで、ステップＳ１２の処理の説明の前に、図３４のステップＳ３１における相互認証処理（なりすましがないことを確認する処理）について、１つの共通鍵を用いる場合（図３５）、２つの共通鍵を用いる場合（図３６）、および公開鍵暗号を用いる場合（図３７）を例として説明する。

【０１５３】

図３５は、１つの共通鍵で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ４１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する（乱数生成部３５が生成するようにしてもよい）。ステップＳ４２において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて乱数Ｒ１を、予め記憶している共通鍵Ｋcで暗号化する（暗号化部３６で暗号化するようにしてもよい）。ステップＳ４３において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ１をEMDサービスセンタ１の相互認証部１７に送信する。

【０１５４】

ステップＳ４４において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ１を予め記憶している共通鍵Ｋcで復号する。ステップＳ４５において

、EMDサービスセンタ１の相互認証部１７は、３２ビットの乱数Ｒ２を生成する。ステップＳ４６において、EMDサービスセンタ１の相互認証部１７は、復号した６４ビットの乱数Ｒ１の下位３２ビットを乱数Ｒ２で入れ替え、連接$R1_H \| R2$を生成する。なお、ここでRi_Hは、Ｒｉの上位ビットを表し、Ａ‖Ｂは、ＡとＢの連接（ｎビットのＡの下位に、ｍビットのＢを結合して、（ｎ＋ｍ）ビットとしたもの）を表す。ステップＳ４７において、EMDサービスセンタ１の相互認証部１７は、DESを用いて$R1_H \| R2$を共通鍵Ｋｃで暗号化する。ステップＳ４８において、EMDサービスセンタ１の相互認証部１７は、暗号化した$R1_H \| R2$をコンテンツプロバイダ２に送信する。

【０１５５】

ステップＳ４９において、コンテンツプロバイダ２の相互認証部３９は、受信した$R1_H \| R2$を共通鍵Ｋｃで復号する。ステップＳ５０において、コンテンツプロバイダ２の相互認証部３９は、復号した$R1_H \| R2$の上位３２ビット$R1_H$を調べ、ステップＳ４１で生成した、乱数Ｒ１の上位３２ビット$R1_H$と一致すれば、EMDサービスセンタ１が正当なセンタであることを認証する。生成した乱数$R1_H$と、受信した$R1_H$が一致しないとき、処理は終了される。両者が一致するとき、ステップＳ５１において、コンテンツプロバイダ２の相互認証部３９は、３２ビットの乱数Ｒ３を生成する。ステップＳ５２において、コンテンツプロバイダ２の相互認証部３９は、受信し、復号した３２ビットの乱数Ｒ２を上位に設定し、生成した乱数Ｒ３をその下位に設定し、連接Ｒ２‖Ｒ３とする。ステップＳ５３において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて連接Ｒ２‖Ｒ３を共通鍵Ｋｃで暗号化する。ステップＳ５４において、コンテンツプロバイダ２の相互認証部３９は、暗号化された連接Ｒ２‖Ｒ３をEMDサービスセンタ１の相互認証部１７に送信する。

【０１５６】

ステップＳ５５において、EMDサービスセンタ１の相互認証部１７は、受信した連接Ｒ２‖Ｒ３を共通鍵Ｋｃで復号する。ステップＳ５６において、EMDサービスセンタ１の相互認証部１７は、復号した連接Ｒ２‖Ｒ３の上位３２ビットを調べ、乱数Ｒ２と一致すれば、コンテンツプロバイダ２を正当なプロバイダとして

認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

【０１５７】

図３６は、２つの共通鍵Ｋｃ１，Ｋｃ２で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ６１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する。ステップＳ６２において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で暗号化する。ステップＳ６３において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ１をEMDサービスセンタ１に送信する。

【０１５８】

ステップＳ６４において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で復号する。ステップＳ６５において、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ１を予め記憶している共通鍵Ｋｃ２で暗号化する。ステップＳ６６において、EMDサービスセンタ１の相互認証部１７は、６４ビットの乱数Ｒ２を生成する。ステップＳ６７において、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ２を共通鍵Ｋｃ２で暗号化する。ステップＳ６８において、EMDサービスセンタ１の相互認証部１７は、暗号化された乱数Ｒ１および乱数Ｒ２をコンテンツプロバイダ２の相互認証部３９に送信する。

【０１５９】

ステップＳ６９において、コンテンツプロバイダ２の相互認証部３９は、受信した乱数Ｒ１および乱数Ｒ２を予め記憶している共通鍵Ｋｃ２で復号する。ステップＳ７０において、コンテンツプロバイダ２の相互認証部３９は、復号した乱数Ｒ１を調べ、ステップＳ６１で生成した乱数Ｒ１（暗号化する前の乱数Ｒ１）と一致すれば、EMDサービスセンタ１を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップＳ７１において、コンテンツプロバイダ２の相互認証部３９は、復号して得た乱数Ｒ２を共通鍵Ｋｃ１で暗号化する。ステップＳ７２において、コンテンツプロバイダ２の相互認

証部３９は、暗号化された乱数Ｒ２をEMDサービスセンタ１に送信する。

【０１６０】

ステップＳ７３において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ２を共通鍵Ｋｃ１で復号する。ステップＳ７４において、EMDサービスセンタ１の相互認証部１７は、復号した乱数Ｒ２が、ステップＳ６６で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、コンテンツプロバイダ２を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

【０１６１】

図３７は、公開鍵暗号である、１６０ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ８１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する。ステップＳ８２において、コンテンツプロバイダ２の相互認証部３９は、自分自身の公開鍵Ｋｐｃｐを含む証明書（認証局から予め取得しておいたもの）と、乱数Ｒ１をEMDサービスセンタ１の相互認証部１７に送信する。

【０１６２】

ステップＳ８３において、EMDサービスセンタ１の相互認証部１７は、受信した証明書の署名（認証局の秘密鍵Ｋｓｃａで暗号化されている）を、予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、コンテンツプロバイダ２の公開鍵Ｋｐｃｐとコンテンツプロバイダ２の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ２の公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ２の公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵Ｋｐｃｐが改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しな

いときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

【０１６３】

適正な認証結果が得られたとき、ステップＳ８４において、EMDサービスセンタ１の相互認証部１７は、６４ビットの乱数Ｒ２を生成する。ステップＳ８５において、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ１および乱数Ｒ２の連接Ｒ１‖Ｒ２を生成する。ステップＳ８６において、EMDサービスセンタ１の相互認証部１７は、連接Ｒ１‖Ｒ２を自分自身の秘密鍵Ｋｓｅｓｃで暗号化する。ステップＳ８７において、EMDサービスセンタ１の相互認証部１７は、連接Ｒ１‖Ｒ２を、ステップＳ８３で取得したコンテンツプロバイダ２の公開鍵Ｋｐｃｐで暗号化する。ステップＳ８８において、EMDサービスセンタ１の相互認証部１７は、秘密鍵Ｋｓｅｓｃで暗号化された連接Ｒ１‖Ｒ２、公開鍵Ｋｐｃｐで暗号化された連接Ｒ１‖Ｒ２、および自分自身の公開鍵Ｋｐｅｓｃを含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ２の相互認証部３９に送信する。

【０１６４】

ステップＳ８９において、コンテンツプロバイダ２の相互認証部３９は、受信した証明書の署名を予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、正しければ証明書から公開鍵Ｋｐｅｓｃを取り出す。この場合の処理は、ステップＳ８３における場合と同様であるので、その説明は省略する。ステップＳ９０において、コンテンツプロバイダ２の相互認証部３９は、EMDサービスセンタ１の秘密鍵Ｋｓｅｓｃで暗号化されている連接Ｒ１‖Ｒ２を、ステップＳ８９で取得した公開鍵Ｋｐｅｓｃで復号する。ステップＳ９１において、コンテンツプロバイダ２の相互認証部３９は、自分自身の公開鍵Ｋｐｃｐで暗号化されている連接Ｒ１‖Ｒ２を、自分自身の秘密鍵Ｋｓｃｐで復号する。ステップＳ９２において、コンテンツプロバイダ２の相互認証部３９は、ステップＳ９０で復号された連接Ｒ１‖Ｒ２と、ステップＳ９１で復号された連接Ｒ１‖Ｒ２を比較し、一致すればEMDサービスセンタ１を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

【０１６５】

適正な認証結果が得られたとき、ステップＳ９３において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ３を生成する。ステップＳ９４において、コンテンツプロバイダ２の相互認証部３９は、ステップＳ９０で取得した乱数Ｒ２および生成した乱数Ｒ３の連接Ｒ２‖Ｒ３を生成する。ステップＳ９５において、コンテンツプロバイダ２の相互認証部３９は、連接Ｒ２‖Ｒ３を、ステップＳ８９で取得した公開鍵Ｋｐｅｓｃで暗号化する。ステップＳ９６において、コンテンツプロバイダ２の相互認証部３９は、暗号化した連接Ｒ２‖Ｒ３をEMDサービスセンタ１の相互認証部１７に送信する。

【０１６６】

ステップＳ９７において、EMDサービスセンタ１の相互認証部１７は、暗号化された連接Ｒ２‖Ｒ３を自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ９８において、EMDサービスセンタ１の相互認証部１７は、復号した乱数Ｒ２が、ステップＳ８４で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、コンテンツプロバイダ２を適正なプロバイダとして認証し、一致しなければ、不適正なプロバイダとして、処理を終了する。

【０１６７】

以上のように、EMDサービスセンタ１の相互認証部１７とコンテンツプロバイダ２の相互認証部３９は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵Ｋｔｅｍｐとして利用される。

【０１６８】

次に、図３３のステップＳ１２の処理について説明する。ステップＳ１２においては、コンテンツプロバイダセキュアコンテナが、コンテンツプロバイダ２からサービスプロバイダ３に供給される処理が行われる。その処理の詳細は、図３８のフローチャートに示されている。すなわち、ステップＳ２０１において、コンテンツプロバイダ２のウォータマーク付加部３２（図８）は、コンテンツサーバ３１からコンテンツＡを読み出し、コンテンツプロバイダ２を示す所定のウォータマーク（電子透かし）を挿入し、圧縮部３３に供給する。

【０１６９】

ステップＳ２０２において、コンテンツプロバイダ２の圧縮部３３は、ウォータマークが挿入されたコンテンツＡをATRAC2等の所定の方式で圧縮し、暗号化部３４に供給する。ステップＳ２０３において、乱数発生部３５は、コンテンツ鍵ＫｃｏＡとなる乱数を発生させ、暗号化部３４に供給する。

【０１７０】

ステップＳ２０４において、コンテンツプロバイダ２の暗号化部３４は、DESなどの所定の方式で、乱数発生部３５で発生された乱数（コンテンツ鍵ＫｃｏＡ）を使用して、ウォータマークが挿入されて圧縮されたコンテンツＡを暗号化する。次に、ステップＳ２０５において、暗号化部３６は、DESなどの所定の方式で、EMDサービスセンタ１から供給された配送用鍵Ｋｄでコンテンツ鍵ＫｃｏＡを暗号化する。

【０１７１】

ステップＳ２０６において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、およびポリシー記憶部３７に記憶されている、コンテンツＡに対応するUCPA，Ｂ（図９）の全体にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵Ｋｓｃｐで暗号化する。これにより、図１４に示した署名が作成される。

【０１７２】

ステップＳ２０７において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、UCPA，Ｂ（図９）、およびステップＳ２０６で生成した署名を含んだ、図１４に示したコンテンツプロバイダセキュアコンテナを作成する。

【０１７３】

ステップＳ２０８において、コンテンツプロバイダ２の相互認証部３９は、サービスプロバイダ３の相互認証部４５（図１６）と相互認証する。この認証処理は、図３５乃至図３７を参照して説明した場合と同様であるので、その説明は省略する。ステップＳ２０９において、コンテンツプロバイダ２のセキュアコンテ

ナ作成部３８は、認証局から予め発行された証明書（図１５）を、ステップＳ２０７で作成したコンテンツプロバイダセキュアコンテナに付して、サービスプロバイダ３に送信する。

【０１７４】

このようにして、コンテンツプロバイダセキュアコンテナが、サービスプロバイダ３に供給されたとき、処理は終了し、図３３のステップＳ１３に進む。

【０１７５】

ステップＳ１３において、サービスプロバイダセキュアコンテナが、サービスプロバイダ３からユーザホームネットワーク５（レシーバ５１）に供給される。この処理の詳細は、図３９のフローチャートに示されている。すなわち、ステップＳ２２１において、サービスプロバイダ３の値付け部４２（図１６）は、コンテンツプロバイダ２から送信されたコンテンツプロバイダセキュアコンテナに付された証明書（図１５）に含まれる署名を確認し、証明書の改竄がなければ、それから、コンテンツプロバイダ２の公開鍵Ｋｐｃｐを取り出す。証明書の署名の確認は、図３７のステップＳ８３における処理と同様であるので、その説明は省略する。

【０１７６】

ステップＳ２２２において、サービスプロバイダ３の値付け部４２は、コンテンツプロバイダ２から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ２の公開鍵Ｋｐｃｐで復号し、得られたハッシュ値が、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、およびUCPA，Ｂの全体にハッシュ関数を適用して得られたハッシュ値と一致するか否かを判定し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。両者の値が一致しない場合（改竄が発見された場合）は、処理は終了されるが、この例の場合、コンテンツプロバイダセキュアコンテナの改竄はなかったものとし、ステップＳ２２３に進む。

【０１７７】

ステップＳ２２３において、サービスプロバイダ３の値付け部４２は、コンテ

ンツプロバイダセキュアコンテナから、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、および署名を取り出し、コンテンツサーバ４１に供給する。コンテンツサーバ４１は、それらを記憶する。値付け部４２はまたUCPA，Ｂも、コンテンツプロバイダセキュアコンテナから取り出し、セキュアコンテナ作成部４４に供給する。

【０１７８】

ステップＳ２２４において、サービスプロバイダ３の値付け部４２は、取り出したUCPA，Ｂに基づいて、PTA－１，Ａ－２（図１７）、およびPTＢ－１，Ｂ－２（図１９）を作成し、セキュアコンテナ作成部４４に供給する。

【０１７９】

ステップＳ２２５において、サービスプロバイダ３のセキュアコンテナ作成部４４は、コンテンツサーバ４１から読み出したコンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、およびコンテンツプロバイダ２の署名、値付け部４２から供給された、UCPA，Ｂ、およびPTＡ－１，Ａ－２，Ｂ－１，Ｂ－２、並びにその署名から、図２１に示したサービスプロバイダセキュアコンテナを作成する。

【０１８０】

ステップＳ２２６において、サービスプロバイダ３の相互認証部４５は、レシーバ５１の相互認証モジュール７１（図２３）と相互認証する。この認証処理は、図３５乃至図３７を参照して説明した場合と同様であるので、その説明を省略する。

【０１８１】

ステップＳ２２７において、サービスプロバイダ３のセキュアコンテナ作成部４４は、ステップＳ２２５で作成したサービスプロバイダセキュアコンテナに、サービスプロバイダ３の証明書（図２２）を付して、ユーザホームネットワーク５のレシーバ５１に送信する。

【０１８２】

このようにして、サービスプロバイダセキュアコンテナが、サービスプロバイ

ダ３からレシーバ５１に送信されたとき、処理は終了し、図３３のステップＳ１４に進む。

【０１８３】

ステップＳ１４において、サービスプロバイダ３から送信されたサービスプロバイダセキュアコンテナが、ユーザホームネットワーク５のレシーバ５１により受信される。この処理の詳細は、図４０のフローチャートに示されている。すなわち、ステップＳ２４１において、レシーバ５１の相互認証モジュール７１（図２３）は、通信部６１を介して、サービスプロバイダ３の相互認証部４５（図１６）と相互認証し、相互認証できたとき、通信部６１は、相互認証したサービスプロバイダ３－１から、サービスプロバイダセキュアコンテナ（図２１）を受信する。相互認証できなかった場合、処理は終了されるが、この例の場合、相互認証されたものとし、ステップＳ２４２に進む。

【０１８４】

ステップＳ２４２において、レシーバ５１の通信部６１は、ステップＳ２４１で相互認証したサービスプロバイダ３から、公開鍵証明書を受信する。

【０１８５】

ステップＳ２４３において、レシーバ５１の復号／暗号化モジュール７４は、ステップＳ２４１で受信したサービスプロバイダセキュアコンテナに含まれる署名を検証し、改竄がなかったか否かを検証する。ここで、改竄が発見された場合、処理は終了するが、この例の場合、改竄が発見されなかったものとし、ステップＳ２４４に進む。

【０１８６】

ステップＳ２４４において、レシーバ５１の記憶モジュール７３に記憶されている基準情報５１（図２９）が、利用条件を満たすUCPと価格条件を満たすPTが選択され、表示制御部６７を介して、図示せず表示部に表示される。ユーザは、表示されたUCPおよびPTの内容を参照して、図示せぬ操作部を操作し、UCPの１つの利用内容を選択する。これにより、入力制御部６８は、操作部から入力された、ユーザの操作に対応する信号をSAM６２に出力する。

【０１８７】

この例の場合、レシーバ５１の基準情報５１の「利用ポイント情報」には、利用ポイントが２２２ポイントであるとされているものとする。すなわち、コンテンツＡに対応して設定されたUCPA，Ｂのうち、「利用条件１０」の「ユーザ条件１０」が”２００ポイント以上”とされている、UCPAが選択される。また、基準情報５１の「決済ユーザ情報」には、ユーザは男性とされているので、PTA－１（図１７（Ａ））の「価格条件１０」に設定された条件を満たす。その結果、UCPAに対応して作成されたPTA－１，PTA－２のうち、PTA－１が選択される。結局、UCPAおよびPTA－１の内容が、表示部に表示される。また、この例の場合、これにより、ユーザが、UCPAの利用内容１１（PTA－１の価格内容１１）を選択したものとする。

【０１８８】

ステップＳ２４５において、レシーバ５１のSAM６２の課金処理モジュール７２は、ステップＳ２４４で選択された、UCPAの「利用内容１１」の内容（PTA－１の「価格内容１１」の内容）に基づいて、UCSA（図２５）および課金情報Ａ（図２７）を作成する。すなわち、この場合、コンテンツＡは、料金が２０００円で買い取り再生される。

【０１８９】

ステップＳ２４６において、サービスプロバイダセキュアコンテナ（図２１）に含まれる、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、UCPA、PTA－１，Ａ－２、およびコンテンツプロバイダ２の署名が取り出され、HDD５２に出力され、記憶される。ステップＳ２４７において、復号／暗号化ユニット７４の復号ユニット９１は、サービスプロバイダセキュアコンテナに含まれるコンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）を、記憶モジュール７３に記憶されている配送用鍵Ｋｄで復号する。

【０１９０】

ステップＳ２４８において、復号／暗号化ユニット７４の暗号化ユニット９３は、ステップＳ２４７で復号されたコンテンツ鍵ＫｃｏＡを、記憶モジュール７３に記憶されている保存用鍵Ｋｓａｖｅで暗号化する。

【０１９１】

ステップＳ２４９において、SAM６２のデータ検査モジュール７５は、ステップＳ２４８で保存用鍵Ｋｓａｖｅで暗号化されたコンテンツ鍵ＫｃｏＡ、およびステップＳ２４５で作成されたUCSAが対応して記憶される、外部記憶部６３の利用情報記憶部６３Ａ（図２６）のブロックBPを検出する。この例の場合、利用情報記憶部６３AのブロックBP－１が検出される。なお、図２６の利用情報記憶部６３Ａにおいて、そのブロックBP－１の利用情報用メモリ領域RP－３にコンテンツ鍵ＫｃｏAおよびUCSAが記憶されているように示されているが、この例の場合、この時点において、それらは記憶されておらず、ブロックBP－１の利用情報用メモリ領域RP－３は、空いており、所定の初期情報が記憶されているものとする。

【０１９２】

ステップＳ２５０において、レシーバ５１のデータ検査モジュール７５は、ステップＳ２４９で検出したブロックBP－１のデータ（利用情報用メモリ領域RP－１乃至RP－Nに記憶されている全てのデータ）にハッシュ関数を適用して、ハッシュ値を得る。次に、ステップＳ２５１において、データ検査モジュール７５は、ステップＳ２５０で得られたハッシュ値と、記憶モジュール７３に記憶されているブロックBP－１に対応する検査値HP－１（図２８）とを比較し、一致するか否かを判定し、一致すると判定した場合、そのブロックBP－１のデータは改竄されていないので、ステップＳ２５２に進む。

【０１９３】

ステップＳ２５２において、レシーバ５１のSAM６２は、利用情報（ステップＳ２４８で、保存用鍵Ｋｓａｖｅで暗号化されたコンテンツ鍵ＫｃｏＡ、およびステップＳ２４５で作成されたUCSA（図２５））を、図２６に示すように、利用情報記憶部６３Ａ（外部記憶部６３）のブロックBP－１の利用情報用メモリ領域RP－３に記憶させる。

【０１９４】

ステップＳ２５３において、レシーバ５１のデータ検査モジュール７５は、ステップＳ２５２で利用情報が記憶された利用情報用メモリ領域RP－３が属する、利用情報記憶部６３AのブロックBP－１のデータにハッシュ関数を適用し、

ハッシュ値を算出し、ステップＳ２５４において、記憶モジュール７３に記憶されている検査値HP－１に上書きする。ステップＳ２５５において、課金処理モジュール７２は、ステップＳ２４５で作成した課金情報Ａを記憶モジュール７３に記憶させ、処理は終了する。

【０１９５】

ステップＳ２５１において、算出されたハッシュ値と検査値HP－１とが一致しないと判定された場合、ブロックBP－１のデータは改竄されているので、手続きは、ステップＳ２５６に進み、データ検査モジュール７５は、外部記憶部６３の利用情報記憶部６３Ａの全てのブロックBPを調べたか否かを判定し、外部記憶部６３の全てのブロックBPを調べていないと判定した場合、ステップＳ２５７に進み、利用情報記憶部６３Ａの、調べていない（空きを有する他の）ブロックBPを検索し、ステップＳ２５０に戻り、それ以降の処理が実行される。

【０１９６】

ステップＳ２５６において、外部記憶部６３の利用情報記憶部６３Ａの全てのブロックBPが調べられたと判定された場合、利用情報を記憶できるブロックBP（利用情報用メモリ領域RP）は存在しないので、処理は終了する。

【０１９７】

このように、サービスプロバイダセキュアコンテナが、レシーバ５１により受信されると、処理は終了し、図３３のステップＳ１５に進む。

【０１９８】

ステップＳ１５において、供給されたコンテンツＡが、レシーバ５１において利用される。なお、この例の場合、図４０のステップＳ２２４で選択されたUCPＡの利用内容１１によれば、コンテンツＡは、再生して利用される。そこで、ここでは、コンテンツＡの再生処理について説明する。この再生処理の詳細は、図４１のフローチャートに示されている。

【０１９９】

ステップＳ２６１において、レシーバ５１のデータ検査モジュール７５は、図４０のステップＳ２５２で、コンテンツ鍵ＫｃｏＡ（保存用鍵Ｋｓａｖｅで暗号化されている）およびUCSAが記憶された利用情報用メモリ領域ＲＰ－３が属する

、外部記憶部６３の利用情報記憶部６３ＡのブロックＢＰ－１のデータにハッシュ関数を適用してハッシュ値を算出する。

【０２００】

ステップＳ２６２において、レシーバ５１のデータ検査モジュール７５は、ステップＳ２６１において算出したハッシュ値が、図４０のステップＳ２５３で算出し、ステップＳ２５４で記憶モジュール７３に記憶させたハッシュ値（検査値ＨＰ－１）と一致するか否かを判定し、一致すると判定した場合、ブロックＢＰ－１のデータは改竄されていないので、ステップＳ２６３に進む。

【０２０１】

ステップＳ２６３において、UCSA（図２５）の「利用内容」の「パラメータ」に示されている情報に基づいて、コンテンツＡが利用可能か否かが判定される。例えば、「利用内容」の「形式」が、”期間制限再生”とされているUCSにおいては、その「パラメータ」には、その開始期間（時刻）と終了期間（時刻）が記憶されているので、この場合、現在の時刻が、その範囲内にあるか否かが判定される。すなわち、現在時刻が、その範囲内にあるとき、そのコンテンツの利用が可能であると判定され、範囲外にあるとき、利用不可と判定される。また、「利用内容」の「形式」が、所定の回数に限って再生（複製）する利用形式とされているUCSにおいては、その「パラメータ」には、残された利用可能回数が記憶されている。この場合、「パラメータ」に記憶されている利用可能回数が０回でないとき、対応するコンテンツの利用が可能であると判定され、一方、利用可能回数が０回であるとき、利用不可と判定される。

【０２０２】

なお、UCSAの「利用内容」の「形式」は、”買い取り再生”とされているので、この場合、コンテンツＡは、買い取られ、制限なしに再生される。すなわち、UCSAの「利用内容」の「パラメータ」には、コンテンツが利用可能であることを示す情報が設定されている。そのため、この例の場合では、ステップＳ２６３において、コンテンツＡが利用可能であると判定され、ステップＳ２６４に進む。

【０２０３】

ステップＳ２６４において、レシーバ５１の課金モジュール７２は、UCSAを更新する。UCSAには、更新すべき情報は含まれていないが、例えば、「利用内容」の「形式」が所定の回数に限って再生する利用形式とされている場合、その「パラメータ」に記憶されている、再生可能回数が１つだけデクリメントされる。

【０２０４】

次に、ステップＳ２６５において、レシーバ５１のSAM６２は、ステップＳ２６４で更新されたUCSA（実際は、更新されていない）を、外部記憶部６３の利用情報記憶部６３Ａのブロック$BP-1$の利用情報用メモリ領域$RP-3$に記憶させる。ステップＳ２６６において、データ検査モジュール７５は、ステップＳ２６５でUCSAが記憶された、外部記憶部６３の利用情報記憶部６３Ａのブロック$BP-1$のデータにハッシュ関数を適用して、ハッシュ値を算出し、記憶モジュール７３に記憶されている検査値$HP-1$に上書きする。

【０２０５】

ステップＳ２６７において、SAM６２の相互認証モジュール７１と、伸張部６４の相互認証モジュール１０１は、相互認証し、SAM６２および伸張部６４は、一時鍵Ｋｔｅｍｐを共有する。この認証処理は、図３５乃至図３７を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数Ｒ１、Ｒ２、Ｒ３、またはその組み合わせが、一時鍵Ｋｔｅｍｐとして用いられる。

【０２０６】

ステップＳ２６８において、復号／暗号化モジュール７４の復号ユニット９１は、図４０のステップＳ２５２で外部記憶部６３の利用情報記憶部６３Ａのブロック$BP-1$（利用情報用メモリ領域$RP-3$）に記憶されたコンテンツ鍵ＫｃｏＡ（保存用鍵Ｋｓａｖｅで暗号化されている）を、記憶モジュール７３に記憶された保存用鍵Ｋｓａｖｅで復号する。

【０２０７】

次に、ステップＳ２６９において、復号／暗号化モジュール７４の暗号化ユニット９３は、復号されたコンテンツ鍵ＫｃｏＡを一時鍵Ｋｔｅｍｐで暗号化する

。ステップＳ２７０において、SAM６２は、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵ＫｃｏＡを伸張部６４に送信する。

【０２０８】

ステップＳ２７１において、伸張部６４の復号モジュール１０２は、コンテンツ鍵ＫｃｏＡを一時鍵Ｋｔｅｍｐで復号する。ステップＳ２７２において、伸張部６４は、インタフェース６６を介して、HDD５２に記録されたコンテンツＡ（コンテンツ鍵Ｋｃｏで暗号化されている）を受け取る。ステップＳ２７３において、伸張部６４の復号モジュール１０３は、コンテンツＡ（コンテンツ鍵Ｋｃｏで暗号化されている）をコンテンツ鍵ＫｃｏＡで復号する。

【０２０９】

ステップＳ２７４において、伸張部６４の伸張モジュール１０４は、復号されたコンテンツＡをATRAC2などの所定の方式で伸張する。ステップＳ２７５において、伸張部６４のウォータマーク付加モジュール１０５は、伸張されたコンテンツＡにレシーバ５１を特定する所定のウォータマーク（電子透かし）を挿入する。ステップＳ２７６において、コンテンツＡは、図示せぬスピーカなどに出力され、処理は終了する。

【０２１０】

ステップＳ２６２において、ステップＳ２６１において算出されたハッシュ値が、レシーバ５１の記憶モジュール７３に記憶されたハッシュ値と一致しないと判定された場合、またはステップＳ２６３において、コンテンツが利用不可と判定された場合、ステップＳ２７７において、SAM６２は、表示制御部６７を介して、図示せぬ表示部にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

【０２１１】

このようにして、レシーバ５１において、コンテンツＡが再生（利用）されたとき、処理は終了し、図３３の処理も終了する。

【０２１２】

次に、レシーバ５１において計上された課金を決済する場合の処理手順を、図４２のフローチャートを参照して説明する。なお、この処理は、計上された課金

が所定の上限額（正式登録時の上限額または仮登録時の上限額）を越えた場合、または配送用鍵Ｋｄのバージョンが古くなり、例えば、図４０のステップＳ２４７で、コンテンツ鍵Ｋｃｏ（配送用鍵Ｋｄで暗号化されている）を復号することができなくなった場合（サービスプロバイダセキュアコンテナを受信することができなくなった場合）に開始される。

【０２１３】

ステップＳ３０１において、レシーバ５１とEMDサービスセンタ１との相互認証が行われる。この相互認証は、図３５乃至図３７を参照して説明した場合と同様の処理であるので、その説明は省略する。

【０２１４】

次に、ステップＳ３０２において、レシーバ５１のSAM６２は、EMDサービスセンタ１のユーザ管理部１８（図３）に証明書を送信する。ステップＳ３０３において、レシーバ５１のSAM６２は、記憶モジュール７３に記憶されている課金情報を、ステップＳ３０１でEMDサービスセンタ１と共有した一時鍵Ｋｔｅｍｐで暗号化し、配送用鍵Ｋｄのバージョン、対応するUCPとPT、並びに登録リストとともに、EMDサービスセンタ１に送信する。

【０２１５】

ステップＳ３０４において、EMDサービスセンタ１のユーザ管理部１８は、ステップＳ３０３で、レシーバ５１から送信された情報を受信し、復号した後、EMDサービスセンタ１のユーザ管理部１８が、登録リストの「状態フラグ」に”停止”が設定されるべき不正行為がレシーバ５１において存在するか否かを確認する。

【０２１６】

ステップＳ３０５において、EMDサービスセンタ１の課金請求部１９は、ステップＳ３０３で受信された課金情報を解析し、ユーザ（例えば、ユーザＦ）の支払い金額を算出する処理等を行う。次に、ステップＳ３０６において、ユーザ管理部１８は、ステップＳ３０５における処理により、決済が成功したか否かを確認する。

【０２１７】

次に、ステップＳ３０７において、EMDサービスセンタ１のユーザ管理部１８は、ステップＳ３０４における確認結果、およびステップＳ３０６における確認結果に基づいて、レシーバ５１の登録条件を設定し、それに署名を付して、レシーバ５１の登録リストを作成する。

【０２１８】

例えば、ステップＳ３０４で、不正行為が確認された場合、「状態フラグ」には”停止”が設定され、この場合、今後、全ての処理が停止される。すなわち、EMDシステムからのサービスを一切受けることができなくなる。また、ステップＳ３０６で、決済が成功しなかったことが確認された場合、「状態フラグ」には”制限あり”が設定され、この場合、すでに購入したコンテンツを再生する処理は可能とされるが、新たにコンテンツを購入する処理は実行できなくなる。

【０２１９】

次に、ステップＳ３０８に進み、EMDサービスセンタ１のユーザ管理部１８は、最新バージョンの配送用鍵Ｋｄ（３月分の最新バージョンの配送用鍵Ｋｄ）およびステップＳ３０７で作成された登録リストを、一時鍵Ｋｔｅｍｐで暗号化し、レシーバ５１に送信する。

【０２２０】

ステップＳ３０９において、レシーバ５１のSAM６２は、EMDサービスセンタ１から送信された配送用鍵Ｋｄおよび登録リストを、通信部６１を介して受信し、復号した後、記憶モジュール７３に記憶させる。このとき、記憶モジュール７３に記憶されていた課金情報は消去され、登録リストおよび配送用鍵Ｋｄが更新される。また、このとき、受信された登録リストの登録リスト署名が検証され、登録リストが改竄されていないとが確認される。この署名の確認処理は、図３７のステップＳ８３における処理と同様であるので、その説明は省略する。

【０２２１】

次に、レシーバ５１が、レシーバ２０１において計上された課金を決済する場合（代理決済する場合）の処理手順を、図４３乃至図４５のフローチャートを参照して説明する。レシーバ５１が、レシーバ２０１から、代理決済を依頼する所定の信号を受信すると、ステップＳ３２１において、レシーバ５１の相互認証モ

ジュール７１は、レシーバ２０１の相互認証モジュール２２１と相互認証を行う。この相互認証は、図３７を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ５１の相互認証モジュール７１は、レシーバ２０１のSAM２１２のIDを取得し、レシーバ２０１と一時鍵Ｋｔｅｍｐを共有する。

【０２２２】

ステップＳ３２２において、レシーバ５１のSAM６２は、HDD５２に記憶されている登録リストが改竄されているか否かを判定する。具体的には、登録リストの「登録リスト署名」に記憶されている署名が、公開鍵暗号の公開鍵で復号され、その結果（ハッシュ値）と、その登録リストのデータの全体のハッシュ値とが、等しいか否かが判定される。

【０２２３】

ステップＳ３２２で、登録リストが改竄されていないと判定された場合、ステップＳ３２３に進み、レシーバ５１のSAM６２は、レシーバ２０１が、代理決済することができる（代理決済すべき）機器であるか否かを判定する。具体的には、ステップＳ３２１で取得されたSAM２１２のIDが、登録リストの「SAMID」に登録され、そしてそれに対応する「課金機器」に自分自身（SAM６２）が登録されているか否かが判定される。

【０２２４】

ステップＳ３２３において、この例の場合のように、レシーバ２０１が代理決済することができる機器であると判定した場合、レシーバ５１のSAM６２は、ステップＳ３２４に進み、課金情報の提供を要求する所定の信号を通信部６５を介して、レシーバ２０１に送信し、ステップＳ３２５において、レシーバ２０１から送信されてきた課金情報を受信する。

【０２２５】

ステップＳ３２６において、レシーバ５１は、EMDサービスセンタ１と相互認証する。この相互認証は、図３５乃至図３７を参照して説明した場合と同様であるので、その説明は省略する。ステップＳ３２７において、レシーバ５１のSAM６２は、ステップＳ３２５で受信した課金情報、記憶モジュール７３に記憶され

ている配送用鍵Ｋｄのバージョン、またHDD５２に記憶されている登録リストを、一時鍵Ｋｔｅｍｐで暗号化し、EMDサービスセンタ１に送信する。

【０２２６】

ステップＳ３２８において、EMDサービスセンタ１のユーザ管理部１８は、レシーバ５１から送信された情報を受信し、復号した後、EMDサービスセンタ１の監査部２１が、登録リストの「状態フラグ」に”停止”が設定されるべき不正行為が、レシーバ５１において存在するか否かを確認する。

【０２２７】

次に、ステップＳ３２９において、EMDサービスセンタ１のユーザ管理部１８は、ステップＳ３２８での確認結果に基づいて、レシーバ５１に不正行為が存在するか否かを判定し、レシーバ５１に不正行為が存在しないと判定した場合、ステップＳ３３０に進む。

【０２２８】

ステップＳ３３０において、EMDサービスセンタ１の課金請求部１９は、ステップＳ３２８で受信された課金情報を解析し、ユーザの支払い金額を算出する処理等を行う。次に、ステップＳ３３１において、EMDサービスセンタ１のユーザ管理部１８は、ステップＳ３３０における決済の結果に基づいて、レシーバ５１およびレシーバ２０１の登録条件を設定し、登録条件署名および登録リスト署名を付して、それぞれの登録リストを作成する。

【０２２９】

次に、ステップＳ３３２に進み、EMDサービスセンタ１のユーザ管理部１８は、最新バージョンの配送用鍵Ｋｄ、並びにステップＳ３３１で作成されたレシーバ５１の登録リストとレシーバ２０１の登録リストを、一時鍵Ｋｔｅｍｐで暗号化して、レシーバ５１に送信する。

【０２３０】

ステップＳ３３３において、レシーバ５１のSAM６２は、EMDサービスセンタ１から送信された配送用鍵Ｋｄ、並びにレシーバ５１の登録リストとレシーバ２０１の登録リストを受信し、復号すると、ステップＳ３３４において、レシーバ５１の登録リストの、レシーバ２０１のSAM２１２のIDに対応する「状態フラグ」

に、動作制限情報（例えば、”制限あり”または”停止”が）設定されているか否かを判定し、それが設定されていない場合、ステップＳ３３５に進む。

【０２３１】

ステップＳ３３５において、レシーバ５１のSAM６２は、ステップＳ３２５で受信された、レシーバ２０１からの課金情報を消去し、ステップＳ３３６において、配送用鍵Ｋｄおよびレシーバ５１の登録リストを更新する。

【０２３２】

次に、ステップＳ３３７において、レシーバ５１のSAM６２は、レシーバ２０１に対して、相互認証（図３３乃至図３５を参照して説明した処理）を行った後、レシーバ２０１に、レシーバ２０１の登録リストと配送用鍵Ｋｄを一時鍵Ｋｔｅｍｐで暗号化して、送信する。

【０２３３】

ステップＳ３３８において、レシーバ２０１は、レシーバ５１から送信されてきたレシーバ２０１の登録リストおよび配送用鍵Ｋｄを受信し、一時鍵Ｋｔｅｍｐで復号した後、記憶する（更新）する。

【０２３４】

ステップＳ３３４で、「状態フラグ」に動作制限情報が設定されていると判定された場合、ステップＳ３３９に進み、レシーバ５１のSAM６２は、レシーバ２０１に対して、所定の処理（REVOKE処理）を実行し、レシーバ２０１において実行される処理を制限する。

【０２３５】

ステップＳ３２９において、レシーバ５１において不正行為が確認された場合、ステップＳ３４０に進み、EMDサービスセンタ１は、レシーバ５１およびレシーバ２０１に対応する「状態フラグ」の全てに”停止”を設定し、それぞれの登録リストを作成し、ステップＳ３４１において、それらをレシーバ５１に送信する。

【０２３６】

ステップＳ３４２において、レシーバ５１は、EMDサービスセンタ１から送信

された登録リストを受信し、登録リストを更新する。その後、ステップＳ３３９に進み、レシーバ５１は、登録リストの「状態フラグ」に設定された動作制限情報に対応する処理を行う。この場合、配送用鍵Ｋｄは、レシーバ５１およびレシーバ２０１には供給されず、レシーバ５１およびレシーバ２０１は、供給されたコンテンツを再生することができなくなり、その結果、EMDシステムにおけるサービスを一切受けることができなくなる。

【０２３７】

ステップＳ３２２において、登録リストが改竄されていると判定された場合、またステップＳ３２３において、代理決済することができる機器ではないと判定された場合、処理は終了される。

【０２３８】

以上のようにして、レシーバ２０１において計上された課金が、レシーバ５１により代理決済させる。

【０２３９】

図４６は、ユーザホームネットワーク５の他の構成例を表している。なお、図中、図１のユーザホームネットワーク５における場合と対応する部分については、同一の符号を付してある。すなわち、レシーバ２０１に代わり、Ｌ個のレシーバ２５１－１乃至２５１－Ｌ（以下、個々に区別する必要がない場合、単に、レシーバ２５１と称する。他の装置についても同様である）、およびHDD２０２に代わり、Ｌ個のHDD２５２－１乃至２５２－Ｌが設けられている。

【０２４０】

レシーバ２５１－１乃至２５１－Ｌは、レシーバ２０１と同様の構成を有する据え置き型の装置で、それぞれHDD２５２－１乃至２５２－Ｌに接続されている。レシーバ２５１はまた、レシーバ２０１と同様に、コンテンツを購入するための処理を実行することができるが、自分自身で課金を決済することができず、レシーバ５１により代理決済されるようになされている。すなわち、例えば、この場合におけるレシーバ５１の登録リスト（図４７）およびレシーバ２５１－１の登録リスト（図４８）に示すように、レシーバ２５１－ｉ（＝１，２，・・・，Ｌ）のSAMのIDに対応する「購入処理」には、”可”が設定され、「課金処理」

には、”不可”が設定され、そして「課金機器」には”SAM６２のID”が、それぞれ設定されている。

【０２４１】

次に、レシーバ５１が、レシーバ２５１において計上される課金を精算する場合の処理手順を、図４９乃至図５１のフローチャートを参照して説明する。

【０２４２】

ステップＳ３６１において、レシーバ５１のSAM６２は、カウンタｉに初期値１を設定し、ステップＳ３６２において、レシーバ５１の相互認証モジュール７１は、レシーバ２５１－ｉ（＝１，２，・・・，Ｌ）の相互認証モジュール（図示せず）と相互認証する。この相互認証は、図３５乃至図３７を参照して説明した場合と同様であるので、その説明は省略する。

【０２４３】

ステップＳ３６３乃至Ｓ３８３においては、図４３のステップＳ３２２乃至Ｓ３４２における場合と同様の処理が実行されるので、その説明は省略する。

【０２４４】

ステップＳ３７９において、レシーバ２５１－ｉが配送鍵Ｋｄおよび登録リストを更新した後、またはレシーバ５１が、「状態フラグ」に設定された動作制限情報に対応した処理を行った後、ステップＳ３８４に進み、レシーバ５１のSAM６２は、カウンタｉの値が、代理決済すべき機器の数（この例の場合、レシーバ２５１の数Ｌ）と等しいか否かを判定し、等しくないと判定した場合、ステップＳ３８５に進み、カウンタｉの値を１だけ増加させて、ステップＳ３６２に戻る。これにより、次のレシーバ２５１－ｉに対応して、それ以降の処理が実行される。

【０２４５】

ステップＳ３８４において、カウンタｉの値と、代理決済すべき機器の数Ｌとが等しいと判定された場合、処理は終了される。

【０２４６】

ステップＳ３６３において、登録リストが改竄されていると判定された場合、またステップＳ３６４において、代理決済することができる機器ではないと判定

された場合、処理は、ステップＳ３８４に進む。

【０２４７】

以上のようにして、Ｌ個のレシーバ２５１－１乃至２５１－Ｌにおいて、それぞれ計上される課金が、レシーバ５１により代理決済される。なお、以上においては、レシーバ５１が、一度に、レシーバ２５１の全てに対して、代理決済を行う場合を例として説明したが、図４３乃至図４５のフローチャートで説明したように、依頼があった機器に対してのみ代理決済を行うようにすることもできる。

【０２４８】

なお、以上において、図４３のステップＳ３２３および図４９のステップＳ３６３における、登録リストが改竄されているか否かの判定は、「登録リスト署名」に記憶されている署名を確認することで行われたが、入力されたデータを、６４ビットずつのブロックに切り分け、それを順次、処理時間の早いブロック暗号器に入力し、所定の検査用鍵で暗号化してそれを第１の出力とし、その第１び出力を遅延された第２の出力との排他的論理和により、データの改竄を確認するCBC(Cipher Block Chaining)モードを利用することもできる。

【０２４９】

図５２は、ユーザホームネットワーク５の他の構成例を表している。なお、図中、図１のユーザホームネットワーク５における場合と対応する部分については、同一の符号を付してある。すなわち、レシーバ２０１およびHDD２０２に代わり、レシーバ３０１、レシーバ４０１、およびHDD４０２が設けられている。

【０２５０】

図５３は、レシーバ３０１の機能的構成例を表している。レシーバ３０１は、レシーバ２０１のSAM２１２乃至通信部２１５と基本的に同様の機能を有する、SAM３１１乃至通信部３１４を有しているが、レシーバ２０１の、通信部２１１、インタフェース２１６、表示制御部２１７、および入力制御部２１８に対応する機能を有しない、携帯型の機器である。

【０２５１】

レシーバ３０１は、HDDに接続されていないので、コンテンツは、図５４に示すような形態を有する、外部記憶部３１２の利用情報記憶部３１２Ａに、コンテ

ンツ鍵Ｋｃｏ（保存鍵Ｋｓａｖｅで暗号化されている）およびUCSと対応して記憶される。

【０２５２】

図５５に示すようなレシーバ３０１の登録リストは、記憶モジュール３２３に記憶されている。この登録リストの対象SAM情報部には、この登録リストを保有するレシーバ３０１のSAM３１１のIDが（「対象SAMID」の欄に）記憶され、その登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ３０１には、レシーバ５１の１機の機器が接続されているので、自分自身を含む合計値２が（「接続されている機器数」の欄に）記憶されている。リスト部には、図３０のレシーバ５１の登録リストの、レシーバ３０１の登録条件が記憶されているが、この場合、「登録条件署名」および「登録リスト署名」は、削除されている。これは、登録リストの署名の確認後、取り除かれたためで、これにより、記憶モジュール３２３の記憶容量を節約することができる。なお、この例の場合、１つの署名あたり、４０バイトが必要とされる。

【０２５３】

レシーバ３０１は、サービスプロバイダ２およびEMDサービスセンタ１と通信を行うことができないので、コンテンツを購入する処理を行うことができない。そのため、「購入処理」には、”不可”が記憶されている。このように、レシーバ３０１においては、コンテンツの購入がなされないので、課金は計上されない。そのため「課金処理」には”不可”が、そして「課金機器」には、”なし”が記憶される。

【０２５４】

レシーバ３０１は、この例の場合、接続されるレシーバ５１から、コンテンツの供給を受けるようになされているので、「コンテンツ供給機器」には、レシーバ５１のSAM６２のIDが記憶されている。

【０２５５】

「状態フラグ」には、この例の場合”なし”が設定されている。「登録条件署

名」および「登録リスト署名」には、所定の署名が記憶されている。

【０２５６】

図５６は、レシーバ４０１の機能的構成例を表している。レシーバ４０１は、レシーバ２０１のSAM２１２乃至入力制御部２１８と基本的に同様の機能を有する、SAM３１１乃至入力制御部４１７を有しているが、レシーバ２０１の通信部２１１に対応する機能を有しない、据え置き型の機器である。

【０２５７】

HDD４０２には、コンテンツ等の他、図５７に示すような、レシーバ４０１の登録リストが記憶されている。この登録リストの対象SAM情報部には、この登録リストを保有するレシーバ４０１のSAM４１１のIDが（「対象SAMID」の欄に）記憶され、その登録リストの有効期限が記憶され、登録リストのバージョン番号が記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ４０１には、レシーバ５１の１機の機器が接続されているので、自分自身を含む合計値２が（「接続されている機器数」の欄に）記憶されている。

【０２５８】

リスト部の「SAMID」には、レシーバ４０１のSAM４１１のIDが記憶され、「ユーザID」には、レシーバ４０１のユーザのIDが記憶される。レシーバ４０１は、サービスプロバイダ２およびEMDサービスセンタ１と通信を行うことができないので、コンテンツを購入する処理を行うことができない。そのため、「購入処理」には、”不可”が記憶されている。

【０２５９】

レシーバ４０１においては、コンテンツの購入がなされないので、課金は計上されない。そのため「課金処理」には”不可”が、「課金機器」には、”なし”が記憶される。レシーバ４０１は、接続されるレシーバ５１からコンテンツの供給を受けるようになされているので、「コンテンツ供給機器」には、レシーバ５１のSAM６２のIDが記憶されている。

【０２６０】

「状態フラグ」には、この例の場合”なし”が設定されている。「登録条件署名」および「登録リスト署名」には、所定の署名が記憶されている。

【０２６１】

なお、この例の場合、レシーバ５１の登録リストは、図５８に示すように、レシーバ５１の登録リストの他、図５５の登録リストに示されるレシーバ３０１の登録条件、および図５７の登録リストに示されるレシーバ４０１の登録条件が設定されている。

【０２６２】

次に、レシーバ５１が、レシーバ３０１に代わり、コンテンツの購入処理を実行する場合の処理手順を、図５９のフローチャートを参照して説明する。ステップＳ４０１において、レシーバ５１は、レシーバ３０１と相互認証を行う。この相互認証は、図３７を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ５１の相互認証モジュール７１は、レシーバ３０１のSAM３１１のIDを取得し、レシーバ３０１と一時鍵Ｋｔｅｍｐを共有する。

【０２６３】

ステップＳ４０２において、レシーバ５１のSAM６２は、HDD５２に記憶されている登録リストが改竄されているか否かを判定する。具体的には、登録リストの「登録リスト署名」に記憶されている署名が、公開鍵暗号の公開鍵で復号され、それ結果（ハッシュ値）と、その登録リストのデータの全体のハッシュ値とが、等しいか否かが判定される。

【０２６４】

ステップＳ４０２で、登録リストが改竄されていないと判定された場合、ステップＳ４０３に進み、レシーバ５１のSAM６２は、代理購入の依頼があったレシーバ３０１が、代理購入することができる機器であるか否かを判定する。具体的には、ステップＳ４０１で取得されたSAM３１１のIDが、登録リストの「SAMID」に登録され、そしてそれに対応する「コンテンツ供給機器」にSAM６２が登録されているか否かが判定される。この例の場合、レシーバ５１の登録リスト（図５８）の「SAMID」には、レシーバ３０１のSAM３１１のIDが設定され、そしてそれに対応する「コンテンツ供給機器」には、SAM６２のIDが設定されているので、ステップＳ４０３において、レシーバ３０１が、代理購入することができる機器であると判定され、ステップＳ４０４に進む。

【０２６５】

ステップＳ４０４において、レシーバ５１のSAM６２は、代理購入が可能であることを示す所定の信号を、通信部６５を介してレシーバ３０１に送信する。

【０２６６】

レシーバ３０１のSAM３１１は、レシーバ５１から、代理購入が可能であることを示す信号を受信すると、ステップＳ４０５において、レシーバ３０１のデータ検査モジュール３２５は、購入するコンテンツＡを記憶する、外部記憶部３１２の利用情報記憶部３１２ＡのブロックＢPを検出する。

【０２６７】

次に、ステップＳ４０６において、レシーバ３０１のデータ検査モジュール３２５は、ステップＳ４０５で検出した、利用情報記憶部３１２ＡのブロックＢPのデータの全体にハッシュ関数を適用してハッシュ値を算出し、記憶モジュール３２３に記憶されている、検出されたブロックＢPに対応する検査値HPと一致しているか否かを判定する。それらの値が一致すると判定された場合、すなわち、利用情報記憶部３１２Ａの、ステップＳ４０５で検出されたブロックＢPのデータが改竄されていない場合、ステップＳ４０７に進み、SAM３１１は、コンテンツの供給を受け取ることが可能であることを示す所定の信号を、通信部３１４を介して、レシーバ５１に送信する。

【０２６８】

ステップＳ４０８において、レシーバ５１のSAM６２（課金モジュール７２）は、選択されたUCPの「利用内容」とPTに基づいて、UCSおよび課金情報を作成する。具体的には、レシーバ５１の表示制御部６７が、UCPA，Ｂ（図９）、およびPTA－１，Ａ－２（図１７），Ｂ－１，Ｂ－２（図１９）の内容を、図示せぬ表示部に出力し、ユーザに提示する。ユーザは、提示されたこれらの情報から、この例の場合、UCPAの「利用内容１１」およびPTA－１を選択する操作を、図示せぬ操作部に対して行う。これにより、入力制御部６８は、ユーザの操作に対応する信号（UCPAの「利用内容１１」のIDとPTA－１のID）を操作部から受信し、それをSAM６２に出力する。SAM６２の課金モジュール７２は、入力制御部６８からのUCPAの「利用内容１１」のIDとPTA－１のIDに基づいて、UCSAおよび

課金情報Ａを作成する。

【０２６９】

なお、この例の場合、レシーバ３０１は、UCPやPTの内容を表示する表示部や、ユーザが、利用内容等を選択することができる操作部を有していない。そこで、このように、レシーバ３０１に接続され、表示部および操作部を有するレシーバ５１を利用して、ユーザは、UCPの内容やPTを選択する。

【０２７０】

次に、ステップＳ４０９において、レシーバ５１のSAM６２は、ステップＳ４０８で作成した課金情報Ａを記憶モジュール７３に記憶させ、また作成したUCSAを、コンテンツ鍵ＫｃｏＡ、およびその署名とともに一時鍵Ｋｔｅｍｐで暗号化し、レシーバ３０１に送信する。なお、この処理が実行されるタイミングで、HDD５２に記憶されているコンテンツＡも一時鍵Ｋｔｅｍｐで暗号化され、レシーバ３０１に送信される。また、レシーバ５１は、UCSAおよびコンテンツ鍵ＫｃｏＡを、レシーバ３０１に送信した後、消去（破棄）する。これにより、コンテンツＡを利用する権利は、レシーバ３０１のみにより保持されるようになる。

【０２７１】

次に、ステップＳ４１０において、レシーバ３０１のSAM３１１は、ステップＳ４０９でレシーバ５１から送信されてきたUCSA、コンテンツ鍵ＫｃｏＡ、およびその署名、並びにコンテンツＡを受信し、一時鍵Ｋｔｅｍｐで復号する。ステップＳ４１１において、レシーバ３０１の復号／暗号化モジュール３２４は、ステップＳ４１０で受信された署名を確認し、レシーバ５１から送信されてきたデータが改竄されているか否かを判定する。この署名の確認は、図３７のステップＳ８３における処理と同様であるので、その説明は省略する。

【０２７２】

ステップＳ４１１において、レシーバ５１から送信されてきたデータが改竄されていないと判定した場合、ステップＳ４１２に進み、レシーバ３０１のSAM３１１は、ステップＳ４１０で受信されたUCSA、コンテンツ鍵ＫｃｏＡ、およびコンテンツＡを外部記憶部３１２の利用情報記憶部３１２Ａの、ステップＳ４０５で検出されたブロックBPに記憶させる。

【０２７３】

次に、ステップＳ４１３において、レシーバ３０１のデータ検査モジュール３２５は、ステップＳ４１２で、UCSA、コンテンツ鍵ＫｃｏＡ、およびコンテンツＡが記憶された外部記憶部３１２の利用情報記憶部３１２ＡのブロックBPのデータにハッシュ関数を適用して、ハッシュ値を算出する。そして、ステップＳ４１４において、データ検査モジュール３２５は、算出したハッシュ値を、記憶モジュール３２３に記憶されている、ブロックBPに対応する検査値HPに上書きする。

【０２７４】

ステップＳ４０２において、登録リストが改竄されていると判定された場合、ステップＳ４０３において、レシーバ３０１が代理決済すべき機器でないと判定された場合、およびステップＳ４０６において、検出されたブロックBPが改竄されていると判定された場合、処理は終了される。

【０２７５】

ステップＳ４１１において、レシーバ５１からのデータが改竄されていると判定された場合、ステップＳ４１５に進み、レシーバ３０１のSAM３１１は、その旨をレシーバ５１に通知する等の処理を実行する。その後、ステップＳ４０９に戻る。すなわち、これにより、UCSA、コンテンツ鍵ＫｃｏＡ、およびその署名、並びにコンテンツＡが、再度、レシーバ３０１に送信される。なお、この例の場合、レシーバ５１からの、この送信は、予め決められた回数だけ行われるものとし、その回数を越えた場合、処理は終了されるものとする。また、これにより処理が終了された場合、ステップＳ４０９で、レシーバ５１の記憶モジュール７３に記憶された課金情報Ａを削除するようにすることもできるが、課金情報Ａに代理購入処理が成功しなかった（失敗した）回数を設定するようにして、その代理購入処理の失敗回数が所定の回数を超えた場合、登録リストの、レシーバ３０１のSAM３１１のIDに対応する「状態フラグ」に”制限あり”とし、レシーバ３０１において行われる処理を制限するようにすることもできる。

【０２７６】

以上のようにして、レシーバ５１により、レシーバ３０１に対する、コンテン

ツの代理購入が行われるが、課金情報は、レシーバ３０１に供給されずに、レシーバ５１に保持されているので、ここで計上された課金は、レシーバ５１自身の課金として精算される（図４２のフローチャートにより決済される）。

【０２７７】

次に、レシーバ３０１が複数のコンテンツを購入する場合の、レシーバ５１による代理購入処理の処理手順を、図６０のフローチャートを参照して説明する。ステップＳ４３１において、レシーバ３０１と相互認証を行う。この相互認証は、図３７を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ５１の相互認証モジュール７１は、レシーバ３０１のSAM３１１のIDを取得し、レシーバ３０１と一時鍵Ｋｔｅｍｐを共有する。

【０２７８】

ステップＳ４３２乃至Ｓ４３４においては、図５９のステップＳ４０２乃至Ｓ４０４における場合と同様の処理が実行されるので、その説明は省略する。

【０２７９】

ステップＳ４３５において、レシーバ３０１のSAM３１１は、カウンタｊの値を初期値１に設定し、次に、レシーバ３０１のデータ検査モジュール３２５は、コンテンツｊ（＝１，２，３・・・Ｋ）を記憶する、外部記憶部３１２の利用情報記憶部３１１Ａのブロック BPを検出する。

【０２８０】

ステップＳ４３７乃至Ｓ４４６においては、図５９のステップＳ４０６乃至Ｓ４１５における場合と同様の処理が実行されるので、その説明は省略する。

【０２８１】

ステップＳ４４７において、レシーバ３０１のSAM３１１は、カウンタｊの値が、購入したいコンテンツの数Ｋと一致するか否かを判定し、一致しない場合、ステップＳ４４８に進み、カウンタｊの値を１だけ増加させ、ステップＳ４３６に戻る。これにより、次の、代理購入されるコンテンツｊに対応する処理が実行される。

【０２８２】

ステップＳ４４７で、カウンタｊの値が、代理するコンテンツの数Ｋと等しい

と判定された場合、処理は終了される。

【０２８３】

以上のようにして、複数のコンテンツが代理購入される。

【０２８４】

次に、レシーバ３０１が、複数のコンテンツを購入する場合の、レシーバ５１による代理購入処理の他の手順を、図６１のフローチャートを参照して説明する。この例の場合も、図６０における場合と同様に、レシーバ３０１が、Ｋ個のコンテンツを購入するものとする。

【０２８５】

ステップＳ４６１において、レシーバ５１は、レシーバ３０１と相互認証を行う。この相互認証は、図３７を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ５１の相互認証モジュール７１は、レシーバ３０１のSAM３１１のIDを取得し、レシーバ３０１と一時鍵Ｋｔｅｍｐを共有する。

【０２８６】

ステップＳ４６２，Ｓ４６３においては、図５９のステップＳ４０２、Ｓ４０３における場合と同様の処理が実行されるので、その説明は省略する。

【０２８７】

ステップＳ４６３において、レシーバ３０１が、代理購入することができる機器であると判定した場合、レシーバ５１のSAM６２は、コンテンツを記憶することができる記憶容量の通知を要求する所定の信号を、レシーバ３０１に送信する。

【０２８８】

レシーバ５１から送信された、記憶容量の通知を要求する信号を受信すると、ステップＳ４６５において、レシーバ３０１のSAM３１１は、コンテンツを記憶することができる、いわゆる、空いている、外部記憶部３１２の利用情報記憶部３１２Ａ（ブロックＢP）の記憶容量を調査し、それをレシーバ５１に通知する。

【０２８９】

ステップＳ４６６において、レシーバ５１は、ステップＳ４６５で通知された記憶容量に記憶することができるｋ（＝＜Ｋ）個のコンテンツのIDを、レシーバ３０１に通知する。例えば、通知されたレシーバ３０１の外部記憶部３１２の空いている容量が、十分大きい場合、購入したいＫ個のコンテンツの全てのIDが通知され、またその容量が十分大きくない場合、その容量に記憶することができる分だけのコンテンツのIDが通知される。

【０２９０】

ステップＳ４６７において、レシーバ３０１のデータ検査モジュール３２５は、ステップＳ４６６でIDが通信されたｋ個のコンテンツを記憶する、外部記憶部３１２の利用情報記憶部３１２Ａのｋ個のブロックＢＰを検出する。ステップＳ４６８において、レシーバ３０１のデータ検査モジュール３２５は、ステップＳ４６７で検出した利用情報記憶部３１２Ａのｋ個のブロックＢＰのそれぞれのデータにハッシュ関数を適用してハッシュ値を算出し、記憶モジュール３２３に記憶されている、検出されたｋ個のブロックＢＰに対応する検査値ＨＰと一致しているか否かをそれぞれ判定し、ｋ個のブロックＢＰのデータが改竄されているか否かを判定する。

【０２９１】

ステップＳ４６８において、ステップＳ４６７で検出された全てのブロックＢＰのデータが改竄されていないと判定された場合、ステップＳ４６９に進み、レシーバ３０１のSAM３１１は、ステップＳ４６６でIDが通知されたｋ個のコンテンツを受け取ることが可能であることを示す信号を、通信部３１４を介して、レシーバ５１に送信する。

【０２９２】

ステップＳ４７０において、レシーバ５１のSAM６２（課金モジュール７２）は、ｋ個のコンテンツに対応するｋ個のUCSおよびｋ個の課金情報を作成する。なお、ここでの具体的な処理は、図５９のステップＳ４０８における場合と、基本的に同様であるので、その説明は省略する。

【０２９３】

次に、ステップＳ４７１において、レシーバ５１のSAM６２は、作成したｋ個

の課金情報を記憶モジュール７３に記憶させ、また作成したｋ個のUCSを、ｋ個のコンテンツ鍵Ｋｃｏ、およびその署名とともに一時鍵Ｋｔｅｍｐで暗号化し、レシーバ３０１に送信する。なお、この処理が実行されるタイミングで、HDD５２に記憶されているｋ個のコンテンツ（購入される）も一時鍵Ｋｔｅｍｐで暗号化され、レシーバ３０１に送信される。

【０２９４】

次に、ステップＳ４７２において、レシーバ３０１のSAM３１１は、ステップＳ４７１でレシーバ５１から送信されてきたｋ個のUCS、ｋ個のコンテンツ鍵Ｋｃｏ、および署名、並びにｋ個のコンテンツをデータを受信し、一時鍵Ｋｔｅｍｐで復号する。ステップＳ４７３において、レシーバ３０１の復号／暗号化モジュール３２４は、ステップＳ４７２で受信された署名を確認し、レシーバ５１から送信されてきたデータが改竄されているか否かを判定する。この署名の確認は、図３７のステップＳ８３における処理と同様であるので、その説明は省略する。

【０２９５】

ステップＳ４７３において、レシーバ５１から送信されてきたデータが改竄されていないと判定された場合、ステップＳ４７４に進み、レシーバ３０１のSAM３１１は、ステップＳ４７２で受信されたｋ個のUCS、ｋ個のコンテンツ鍵Ｋｃｏ、およびｋ個のコンテンツを外部記憶部３１２の利用情報記憶部３１２Ａの、ステップＳ４６７で検出されたｋ個のブロックBPに記憶させる。

【０２９６】

ステップＳ４７５において、レシーバ３０１のデータ検査モジュール３２５は、ステップＳ４７４で、UCS、コンテンツ鍵Ｋｃｏ、およびコンテンツが記憶された外部記憶部３１２の利用情報記憶部３１２Ａのｋ個のブロックBPのデータにハッシュ関数を適用して、それぞれのハッシュ値を算出し、それを、ステップＳ４７６において、記憶モジュール３２３に記憶されている、対応する検査値HPに上書きする。その後、処理は終了される。

【０２９７】

ステップＳ４６２において、登録リストが改竄されていると判定された場合、

ステップＳ４６３において、レシーバ３０１が代理決済すべき機器でないと判定された場合、およびステップＳ４６８において、検出されたブロックＢＰが改竄されていると判定された場合、処理は終了される。

【０２９８】

ステップＳ４７３において、レシーバ５１からのデータが改竄されていると判定された場合、ステップＳ４７７に進み、レシーバ３０１のSAM３１１は、その旨をレシーバ５１に通知する等の処理を実行する。その後、ステップＳ４７１に戻る。すなわち、これにより、ｋ個のUCS、ｋ個のコンテンツ鍵Ｋｃｏ、およびその署名、並びにｋ個のコンテンツが、再度、レシーバ３０１に送信される。なお、この場合も、レシーバ５１からの、この送信は、予め決められた回数だけ行われるものとし、その回数を越えた場合、処理は終了されるものとする。また、これにより処理が終了された場合、ステップＳ４７１で、レシーバ５１の記憶モジュール７３に記憶されたｋ個の課金情報を削除するようにすることもできるが、ｋ個の課金情報のそれぞれに代理購入処理の失敗回数を設定するようにして、その回数が所定の回数を越えた場合、登録リストの、レシーバ３０１のSAM３１１のIDに対応する「状態フラグ」に”制限あり”とし、レシーバ３０１において行われる処理を制限することもできる。

【０２９９】

次に、レシーバ５１が、レシーバ４０１に代わり、コンテンツを購入する場合（代理購入する場合）の処理手順を、図６２，図６３のフローチャートを参照して説明する。レシーバ５１は、レシーバ４０１から、購入したいコンテンツのIDと、所定の代理購入を依頼する所定の信号を受信すると、ステップＳ５０１において、レシーバ５１は、レシーバ４０１と相互認証を行う。この相互認証は、図３７を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ５１の相互認証モジュール７１は、レシーバ４０１のSAM４１１のIDを取得し、レシーバ４０１と一時鍵Ｋｔｅｍｐを共有する。

【０３００】

ステップＳ５０２において、レシーバ５１のSAM６２は、HDD５２に記憶されている登録リストが改竄されているか否かを判定し、登録リストが改竄されていな

いと判定された場合、ステップＳ５０３に進み、代理購入の依頼のあったレシーバ４０１が、代理購入すべき機器であるか否かを判定する。ここでの具体的な処理は、図５９のステップＳ４０３における場合と同様であるので、その説明は省略する。ステップＳ５０３で、レシーバ４０１が、代理決済すべき機器であると判定した場合、レシーバ５１のSAM６２は、ステップＳ５０４に進み、予め通知された、レシーバ５０１が購入したいコンテンツのUCPおよびPTを、署名を付して、レシーバ４０１に送信する。なお、UCP、PT、およびコンテンツは、サービスプロバイダセキュアコンテナに含まれているので、そのまま渡してもよい。

【０３０１】

ステップＳ５０５において、レシーバ４０１のSAM４１１は、レシーバ５１から送信されたUCP、PT、およびその署名を受信し、ステップＳ５０６において、署名を確認し、レシーバ５１から送信されてきたデータが改竄されているか否かを判定する。この署名の確認は、図３７のステップＳ８３における処理と同様であるので、その説明は省略する。

【０３０２】

ステップＳ５０６において、レシーバ５１から送信されてきたデータが改竄されていないと判定した場合、レシーバ４０１のSAM４１１は、ステップＳ５０７に進み、購入するコンテンツに対応するコンテンツ鍵Ｋｃｏを記憶する、外部記憶部４１２の利用情報記憶部４１２Ａのブロック BP（図示せず）を検出する。

【０３０３】

次に、ステップＳ５０８において、レシーバ４０１のデータ検査モジュール４２５は、ステップＳ５０７で検出された利用情報記憶部４１２Ａのブロック BPに記憶されているデータの全体にハッシュ関数を適用してハッシュ値を算出し、記憶モジュール４２３に記憶されている、検出されたブロック BPに対応する検査値HPと一致するか否かを判定する。それらの値が一致すると判定された場合、すなわち、利用情報記憶部４１２Ａの、検出されたブロック BPが改竄されていない場合、ステップＳ５０９に進む。

【０３０４】

ステップＳ５０９において、レシーバ４０１のSAM４１１は、ステップＳ５０

５で受信されたUCPの「利用内容」とPTのIDをレシーバ５１の通知する。なお、実際は、この処理に先だって、レシーバ４０１の表示制御部４１６が、ステップＳ５０５で受信されたUCPおよびPTの内容を、図示せぬ表示部に出力し、ユーザに提示する。ユーザは、提示されたこれらの情報から、UCPの利用内容およびPTを選択する操作を、図示せぬ操作部に対して行う。これにより、入力制御部４１７は、ユーザの操作に対応する信号（UCPの「利用内容」のIDとPTのID）を操作部から受信し、それをSAM４１１に出力する。SAM４１１は、入力制御部４１７からの情報を、通信部４１４に介してレシーバ５１に送信する。

【０３０５】

このように、ユーザが、UCPの内容およびPTを選択することができる機能を有するレシーバ４０１に対しては、UCPおよびPT（購入するコンテンツのIDおよび選択項目）が、レシーバ５１から送信される。なお、UCPおよびPTに代えて、

ステップＳ５１０において、レシーバ５１のSAM６２は、レシーバ４０１から通知されたUCPの「利用内容」のIDおよびPTのID（購入するコンテンツのIDおよび選択項目）に基づいて、課金情報およびUCSを作成する。次に、ステップＳ５１１において、レシーバ５１のSAM６２は、ステップＳ５１０で作成した課金情報を記憶モジュール７３に記憶させ、そして作成したUCSを、購入されるコンテンツに対応するコンテンツ鍵Ｋｃｏ、およびそれらの署名とともにレシーバ４０１に送信する。なお、この処理が実行されるタイミングで、HDD５２に記憶されている、購入されるコンテンツもレシーバ４０１に送信される。なお、サービスプロバイダセキュアコンテナをレシーバ４０１に送信し、レシーバ４０１が、改竄チェック、利用内容の選択、および要求を出して、レシーバ５１で購入し、UCSや鍵を渡すようにすることもできる。

【０３０６】

次に、ステップＳ５１２において、レシーバ４０１のSAM４１１は、ステップＳ５１１でレシーバ５１から送信されてきたUCS、コンテンツ鍵Ｋｃｏ、およびその署名、並びにコンテンツを受信し、一時鍵Ｋｔｅｍｐで復号する。ステップＳ５１３において、レシーバ４０１の復号／暗号化モジュール４２４は、ステップＳ５１２で受信された署名を確認し、レシーバ５１から送信されてきたデータ

が改竄されているか否かを判定する。この署名の確認は、図３７のステップＳ８３における処理と同様であるので、その説明は省略する。

【０３０７】

ステップＳ５１３において、レシーバ５１から送信されてきたデータが改竄されていないと判定された場合、ステップＳ５１４に進み、レシーバ４０１のSAM４１１は、ステップＳ５０５で受信されたUCP、PT、およびコンテンツをHDD４０２に記憶させる。次に、ステップＳ５１５において、SAM４１１は、ステップＳ５１２で受信されたUCSとコンテンツ鍵Ｋｃｏを、外部記憶部４１２の利用情報記憶部４１２Ａの、ステップＳ５０７で検出されたブロックＢＰに記憶させる。

【０３０８】

次に、ステップＳ５１６において、レシーバ４０１のデータ検査モジュール４２５は、ステップＳ５１５で、UCSとコンテンツ鍵Ｋｃｏが記憶された外部記憶部４１２の利用情報記憶部４１２Ａのブロック ＢＰのデータにハッシュ関数を適用して、ハッシュ値を算出し、それを、ステップＳ５１７において、記憶モジュール４２３に記憶されている、対応する検査値HPに上書きする。

【０３０９】

ステップＳ５０２において、登録リストが改竄されていると判定された場合、ステップＳ５０３において、レシーバ４０１が代理決済すべき機器でないと判定された場合、およびステップＳ５０８において、利用情報が記憶されるブロックＢＰが改竄されていると判定された場合、処理は終了される。

【０３１０】

ステップＳ５０６において、レシーバ５１からのデータが改竄されていると判定された場合、ステップＳ５１８に進み、レシーバ４０１のSAM４１１は、その旨をレシーバ５１に通知する等の処理を実行する。その後、ステップＳ５０４に戻る。すなわち、これにより、UCP、PT、およびその署名が、再度、レシーバ４０１に送信される。なお、この例の場合、レシーバ５１からの、この送信は、予め決められた回数だけ行われるものとし、その回数を越えた場合、処理は終了されるものとする。

【０３１１】

ステップＳ５１３において、レシーバ５１からのデータが改竄されていると判定された場合、ステップＳ５１９に進み、レシーバ４０１のSAM４１１は、その旨をレシーバ５１に通知する等の処理を実行する。その後、ステップＳ５１１に戻る。すなわち、これにより、UCS、コンテンツ鍵Ｋｃｏ、およびその署名、並びにコンテンツが、再度、レシーバ４０１に送信される。なお、この例の場合、レシーバ５１からの、この送信は、予め決められた回数だけ行われるものとし、その回数を越えた場合、処理は終了されるものとする。また、これにより終了された場合、ステップＳ５１０で、レシーバ５１の記憶モジュール７３に記憶された課金情報を削除するようにすることもできるが、課金情報に代理購入処理の失敗回数を設定するようにして、その回数が所定の回数を越えたとき、登録リストのレシーバ４０１のSAM４１１のIDに対応する「状態フラグ」に”制限あり”とし、レシーバ４０１における処理を制限するようにすることもできる。

【０３１２】

なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動画像データ、静止画像データ、文書データ、またはプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であればMPEG(Moving Picture Experts Group)などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

【０３１３】

また、共通鍵暗号は、ブロック暗号であるDESを使用して説明したが、NTT（商標）が提案するFEAL、IDEA(International Data Encription Algorithm)、または１ビット乃至数ビット単位で暗号化するストリーム暗号などでもよい。

【０３１４】

さらに、コンテンツおよびコンテンツ鍵Ｋｃｏの暗号化は、共通鍵暗号方式を利用するとして説明したが、公開鍵暗号方式でもよい。

【０３１５】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【０３１６】

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【０３１７】

【発明の効果】

請求項１に記載の情報処理装置、請求項２に記載の情報処理方法、および請求項３に記載の提供媒体によれば、他の情報処理装置から、課金情報を受信し、管理装置に送信するようにしたので、課金情報に基づいて行われた決済処理に基づいて作成された動作制限情報に基づいて、動作を制御することができる。

【０３１８】

請求項４に記載の情報処理装置、請求項６に記載の情報処理方法、および請求項７に記載の提供媒体によれば、代理購入情報に対応して、使用許諾条件情報を作成し、暗号化された情報を復号するために必要な鍵とともに、他の情報処理装置に送信するようにしたので、他の情報処理装置が、暗号化された情報を復号して利用することができる。

【図面の簡単な説明】

【図１】

EMDシステムを説明する図である。

【図２】

EMDシステムにおける、主な情報の流れを説明する図である。

【図３】

EMDサービスセンタ１の機能的構成を示すブロック図である。

【図４】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図５】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する他の図である。

【図６】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する他の図である。

【図７】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する他の図である。

【図８】

コンテンツプロバイダ２の機能的構成例を示すブロック図である。

【図９】

UCPを説明する図である。

【図１０】

コンテンツの管理移動を説明する図である。

【図１１】

第１世代複製を説明する図である。

【図１２】

サービスコードおよびコンディションコードのコード値の例を示す図である。

【図１３】

UCPの利用条件として設定されたコード値の例を示す図である。

【図１４】

コンテンツプロバイダセキュアコンテナの例を示す図である。

【図１５】

コンテンツプロバイダ２の証明書の例を示す図である。

【図１６】

サービスプロバイダ３の機能の構成を示すブロック図である。

【図１７】

PTの例を示す図である。

【図１８】

PTの価格条件として設定されたコード値の例を示す図である。

【図１９】

他のPTの例を示す図である。

【図２０】

他のPTの価格条件として設定されたコード値の例を示す図である。

【図２１】

サービスプロバイダセキュアコンテナの例を示す図である。

【図２２】

サービスプロバイダ３の証明書の例を示す図である。

【図２３】

ユーザホームネットワーク５のレシーバ５１の機能的構成例を示すブロック図である。

【図２４】

レシーバ５１のSAM６２の証明書の例を示す図である。

【図２５】

UCSの例を示す図である。

【図２６】

レシーバ５１の外部記憶部６３の利用情報記憶部６３Ａの内部を説明する図である。

【図２７】

課金情報の例を示す図である。

【図２８】

レシーバ５１の記憶モジュール７３に記憶されている情報を示す図である。

【図２９】

基準情報５１を説明する図である。

【図３０】

レシーバ５１の登録リストの例を示す図である。

【図３１】

ユーザホームネットワーク５のレシーバ２０１の機能的構成例を示すブロック図である。

【図３２】

レシーバ２０１の登録リストの例を示す図である。

【図３３】

コンテンツの利用処理を説明するフローチャートである。

【図３４】

EMDサービスセンタ１がコンテンツプロバイダ２へ配送用鍵Ｋｄを送信する処

理を説明するフローチャートである。

【図３５】

コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の動作を説明するフローチャートである。

【図３６】

コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の他の動作を説明するフローチャートである。

【図３７】

コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の他の動作を説明するフローチャートである。

【図３８】

コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図３９】

サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図４０】

レシーバ５１がサービスプロバイダセキュアコンテナを受信する処理を説明するフローチャートである。

【図４１】

レシーバ５１がコンテンツを再生する処理を説明するフローチャートである。

【図４２】

課金を決済する処理を説明するフローチャートである。

【図４３】

代理決済処理の手順を説明するフローチャートである。

【図４４】

代理決済処理の手順を説明するフローチャートである。

【図４５】

代理決済処理の手順を説明するフローチャートである。

【図４６】

ユーザホームネットワーク５の他の構成例を示す図である。

【図４７】

ユーザホームネットワーク５のレシーバ５１の登録リストの例を示す図である。

【図４８】

ユーザホームネットワーク５のレシーバ２５１の登録リストの例を示す図である。

【図４９】

代理決済処理の他の手順を説明するフローチャートである。

【図５０】

代理決済処理の他の手順を説明するフローチャートである。

【図５１】

代理決済処理の他の手順を説明するフローチャートである。

【図５２】

ユーザホームネットワーク５の他の構成例を示す図である。

【図５３】

レシーバ３０１の構成例を示す図である。

【図５４】

レシーバ３０１の利用情報記憶部３１２Ａの形態を示す図である。

【図５５】

レシーバ３０１の登録リストの例を示す図である。

【図５６】

レシーバ４０１の構成例を示す図である。

【図５７】

レシーバ４０１の登録リストの例を示す図である。

【図５８】

レシーバ５１の登録リストの例を示す図である。

【図５９】

代理購入処理の手順を説明するフローチャートである。

【図６０】

代理購入処理の他の手順を説明するフローチャートである。

【図６１】

代理購入処理の他の手順を説明するフローチャートである。

【図６２】

代理購入処理の他の手順を説明するフローチャートである。

【図６３】

代理購入処理の他の手順を説明するフローチャートである。

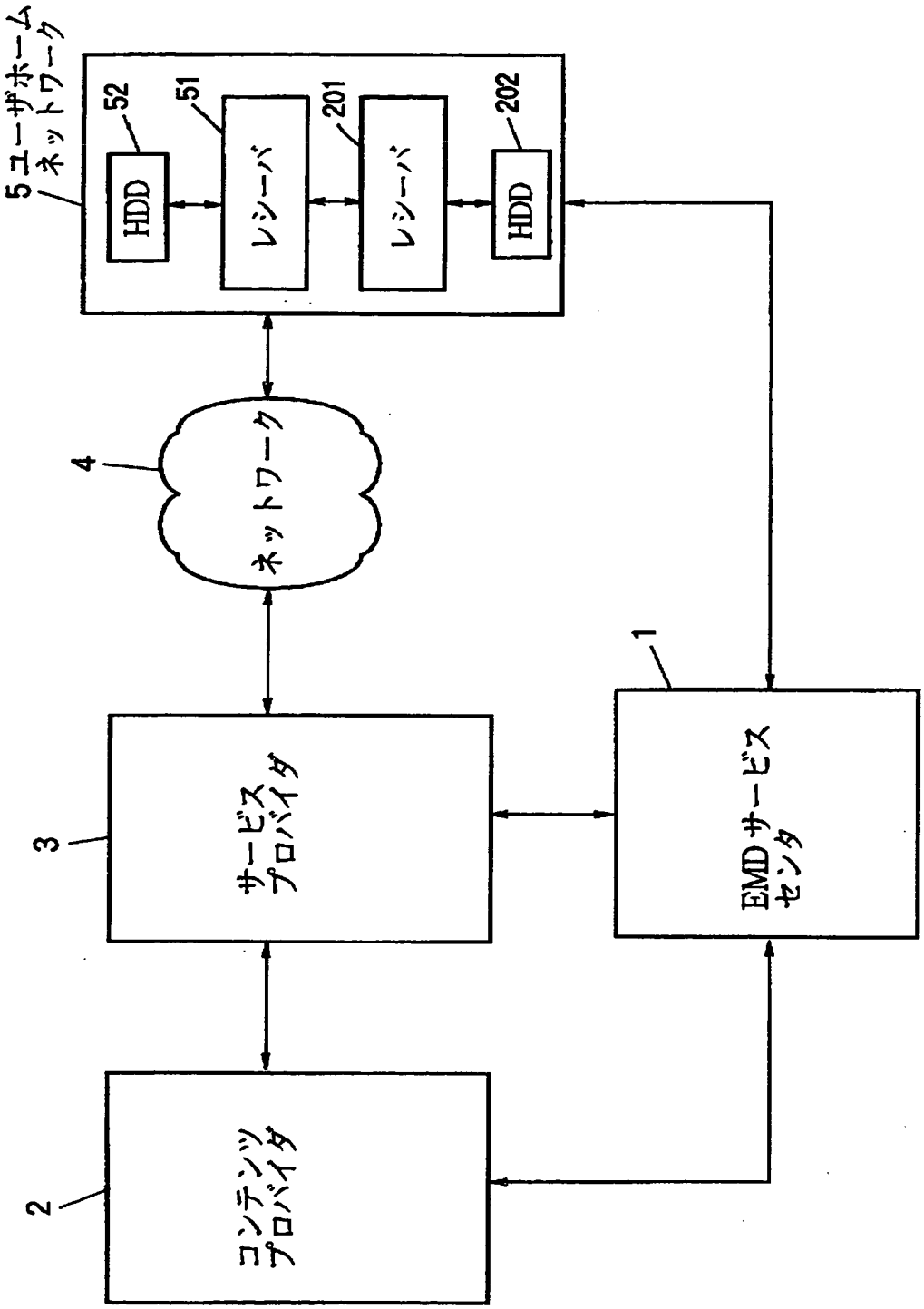
【符号の説明】

１　EMDサービスセンタ，　２　コンテンツプロバイダ，　３　サービスプロバイダ，　５　ユーザホームネットワーク，　１１　サービスプロバイダ管理部，　１２　コンテンツプロバイダ管理部，　１３　著作権管理部，　１４　鍵サーバ，　１５　経歴データ管理部，　１６　利益分配部，　１７　相互認証部，　１８　ユーザ管理部，　１９　課金請求部，　２０　出納部，　２１　監査部，　３１　コンテンツサーバ，　３２　ウォータマーク付加部，　３３　圧縮部，　３４　暗号化部，　３５　乱数発生部，　３６　暗号化部，　３７　ポリシー記憶部，　３８　セキュアコンテナ作成部，　３９　相互認証部，　４１　コンテンツサーバ，　４２　値付け部，　４３　ポリシー記憶部，　４４　セキュアコンテナ作成部，　４５　相互認証部，　５１　レシーバ，　５２　HDD，　６１　通信部，　６２　SAM，　６３　外部記憶部，　６４　伸張部，　６５　通信部，　６６　インタフェース，　６７　表示制御部，　６８　入力制御部，　７１　相互認証モジュール，　７２　課金処理モジュール，　７３　記憶モジュール，　７４　復号／暗号化モジュール，　７５　データ検査モジュール，　９１　復号ユニット，　９２　乱数発生ユニット，　９３　暗号化ユニット，　１０１　相互認証モジュール，　１０２　復号モジュール，　１０３　復号モジュール，　１０４　伸張モジュール，　１０５　ウォータマーク付加モジュール，　２０１　レシーバ，　２０２　HDD，　２１１　通信部，　２１２　SAM，　２１３　外部記憶部，　２１４　伸張部，　２１５　通信部，　２１６　インタ

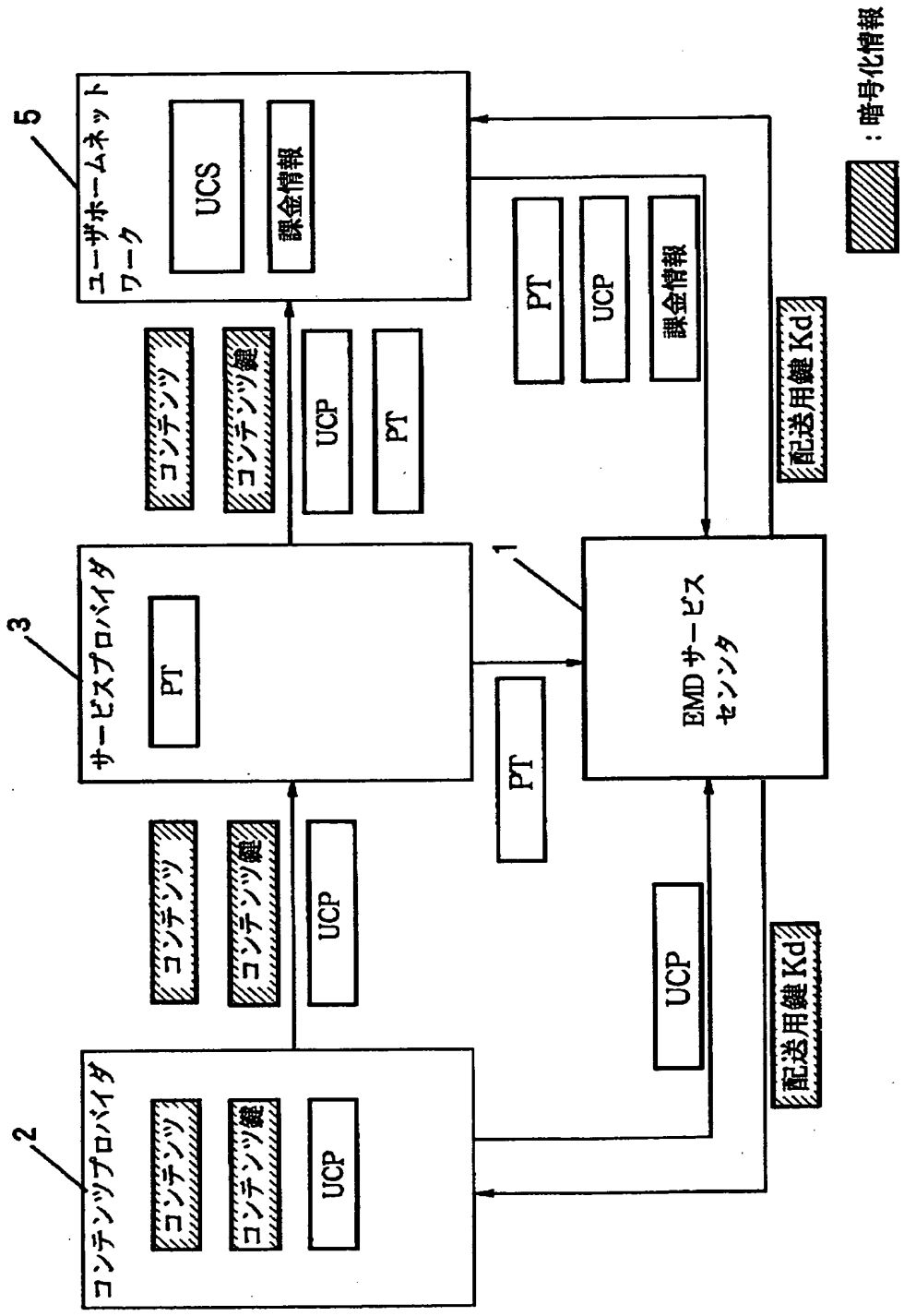
フェース，　２１７　表示制御部，　２１８　入力制御部，　２２１　相互認証モジュール，　２２２　課金処理モジュール，　２２３　記憶モジュール，　２２４　復号／暗号化モジュール，　２２５　データ検査モジュール，　２３１　復号ユニット，　２３２　乱数発生ユニット，　２３３　暗号化ユニット，　２４１　相互認証モジュール，　２４２　復号モジュール，　２４３　復号モジュール，　２４４　伸張モジュール，　２４５　ウォータマーク付加モジュール，　３０１　レシーバ，　３１１　SAM，　３１２　外部記憶部，　３１３　伸張部，　３１４　通信部，　３２１　相互認証モジュール，　３２２　課金処理モジュール，　３２３　記憶モジュール，　３２４　復号／暗号化モジュール，　３２５　データ検査モジュール，　３３１　復号ユニット，　３３２　乱数発生ユニット，　３３３　暗号化ユニット，　３４１　相互認証モジュール，　３４２　復号モジュール，　３４３　復号モジュール，　３４４　伸張モジュール，　３４５　ウォータマーク付加モジュール，　４０１　レシーバ，　４０２　HDD，　４１１　SAM，　４１２　外部記憶部，　４１３　伸張部，　４１４　通信部，　４１５　インタフェース，　４１６　表示制御部，　４１７　入力制御部，　４２１　相互認証モジュール，　４２２　課金処理モジュール，　４２３　記憶モジュール，　４２４　復号／暗号化モジュール，　４２５　データ検査モジュール，　４３１　復号ユニット，　４３２　乱数発生ユニット，　４３３　暗号化ユニット，　４４１　相互認証モジュール，　４４２　復号モジュール，　４４３　復号モジュール，　４４４　伸張モジュール，　４４５　ウォータマーク付加モジュール

【書類名】　図面

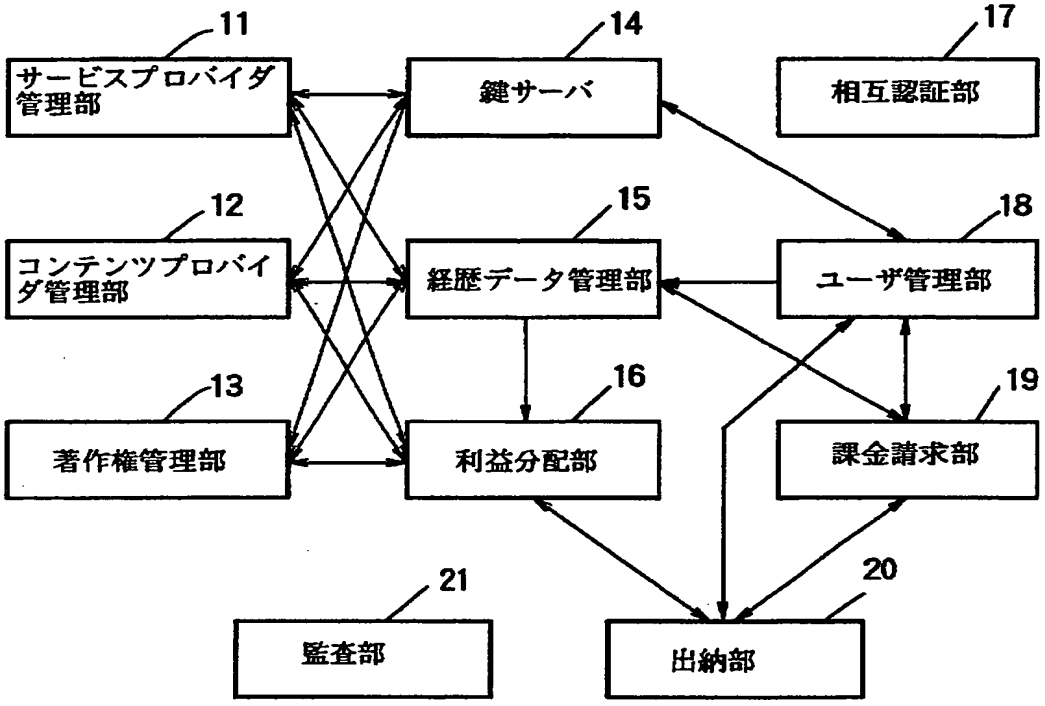
【図１】


5 ユーザホーム ネットワーク
52
51
201
202
HDD
レシーバ
レシーバ
HDD
4
ネットワーク
1
3
サービス プロバイダ
EMD サービス センタ
2
コンテンツ プロバイダ

【図２】

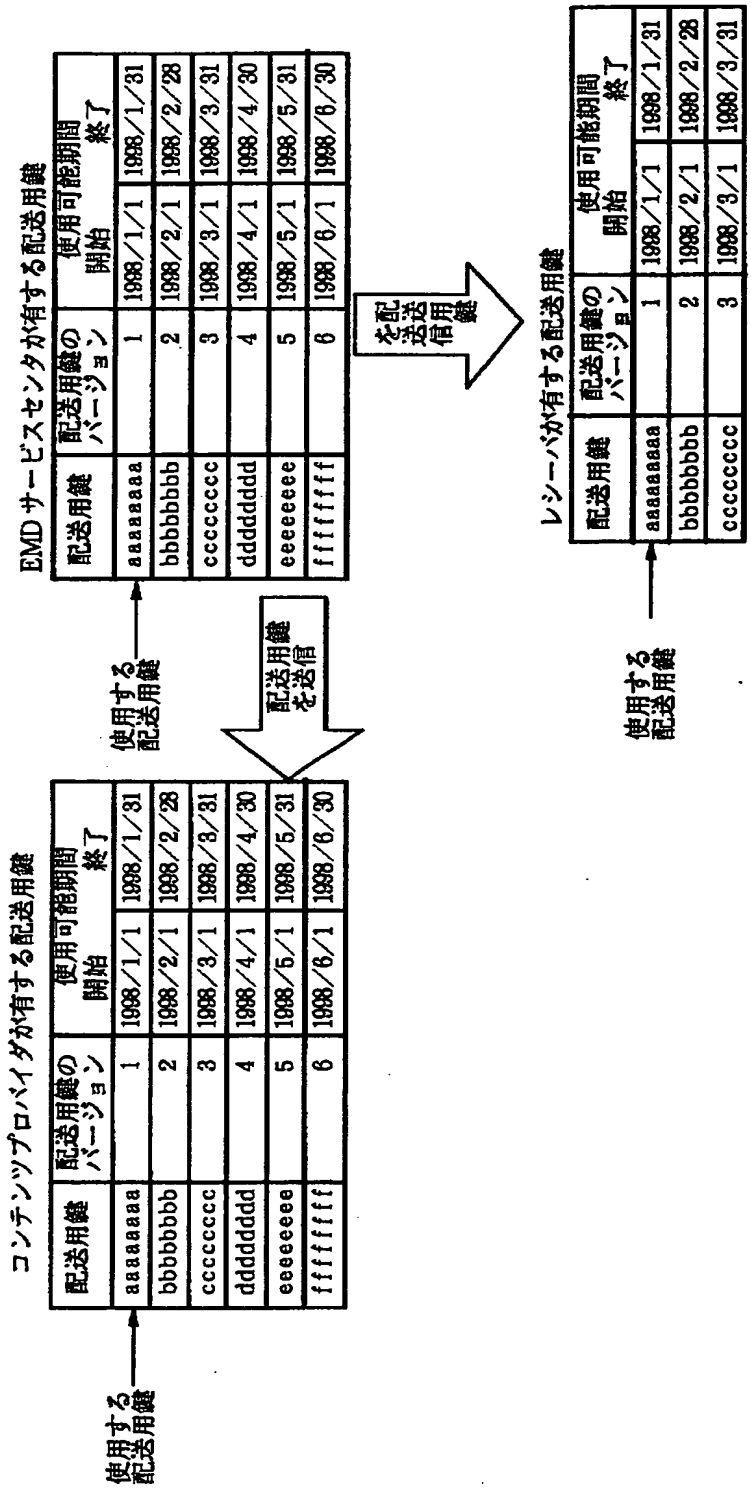

：暗号化情報
5
ユーザホームネットワーク
UCS
課金情報
PT
UCP
課金情報
配送用鍵 Kd
コンテンツ
コンテンツ鍵
UCP
PT
3
サービスプロバイダ
PT
1
EMD サービスセンタ
PT
UCP
配送用鍵 Kd
コンテンツ
コンテンツ鍵
UCP
2
コンテンツプロバイダ
コンテンツ
コンテンツ鍵
UCP

【図３】

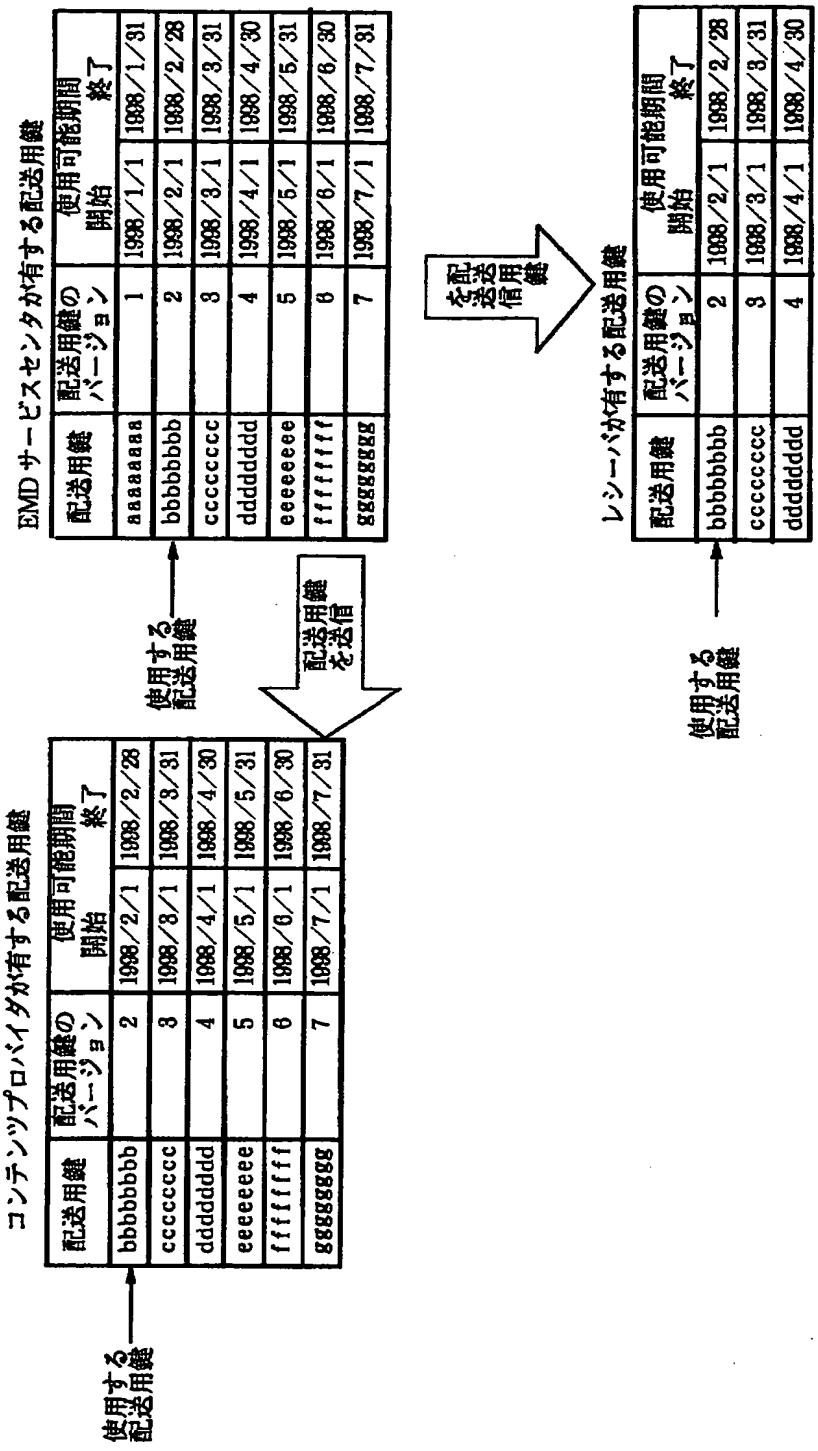


EMD サービスセンタ 1

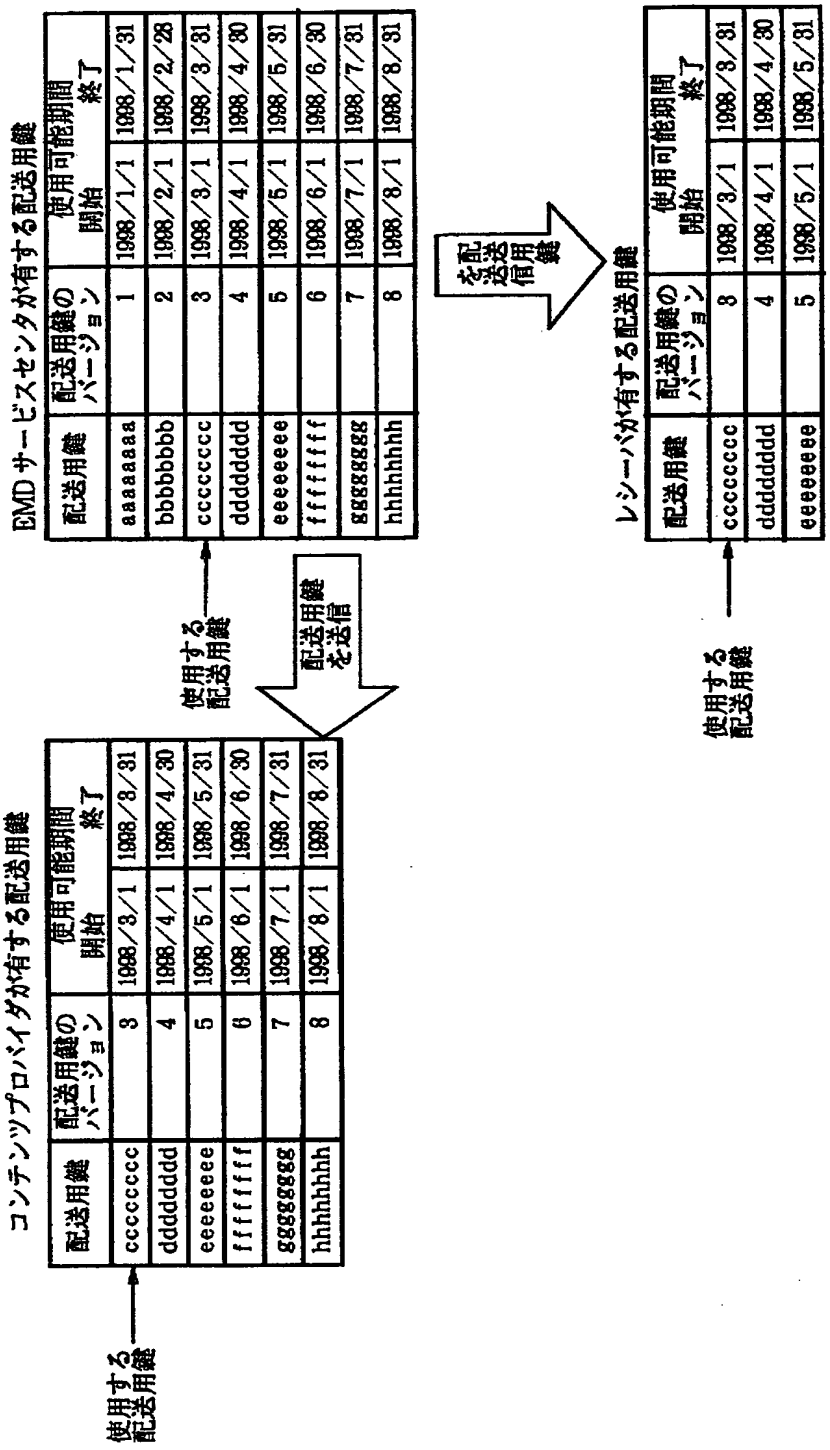
【図４】


コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵
配送用鍵を送信
EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵
を配送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
使用する配送用鍵

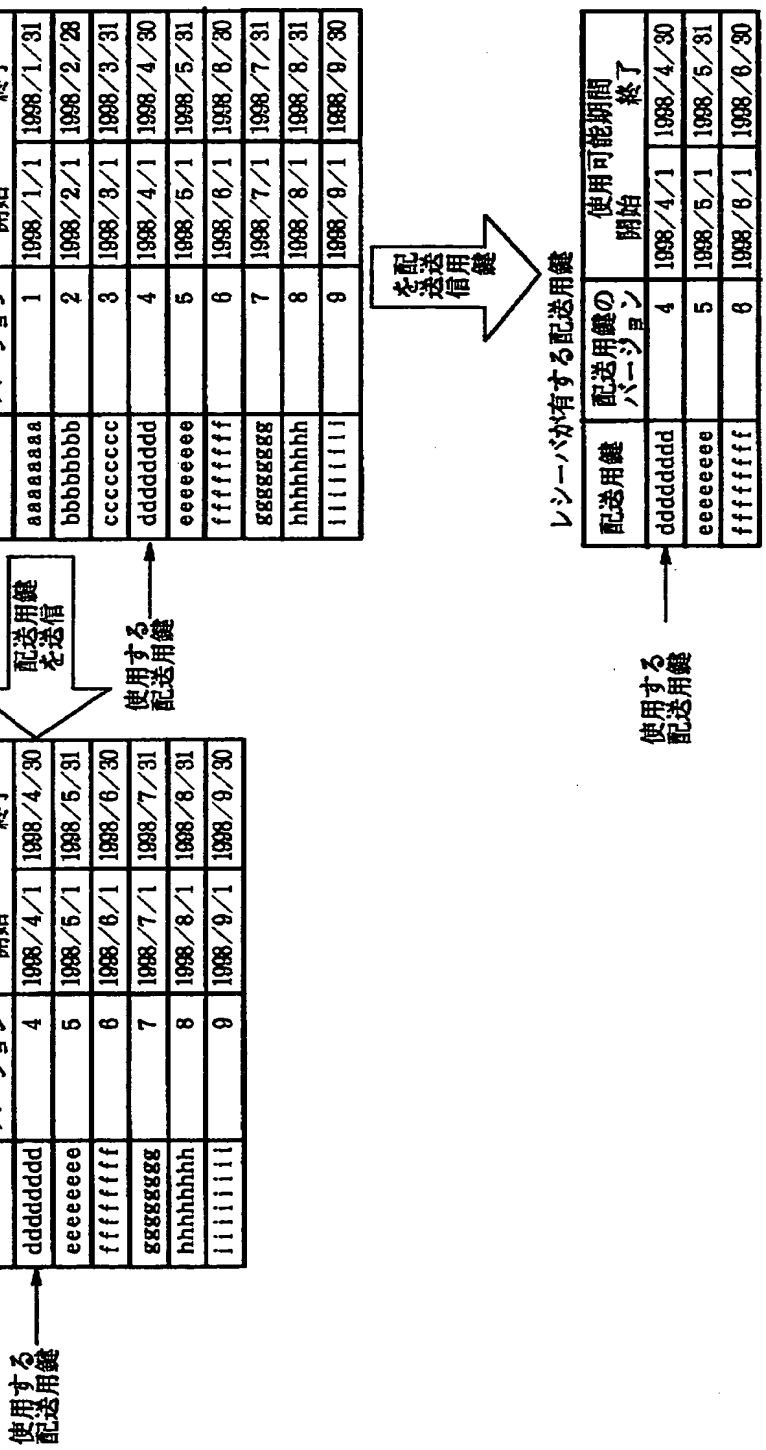
【図５】


EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
使用する配送用鍵
配送用鍵を送信
コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
使用する配送用鍵
配送用鍵を送信
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
使用する配送用鍵

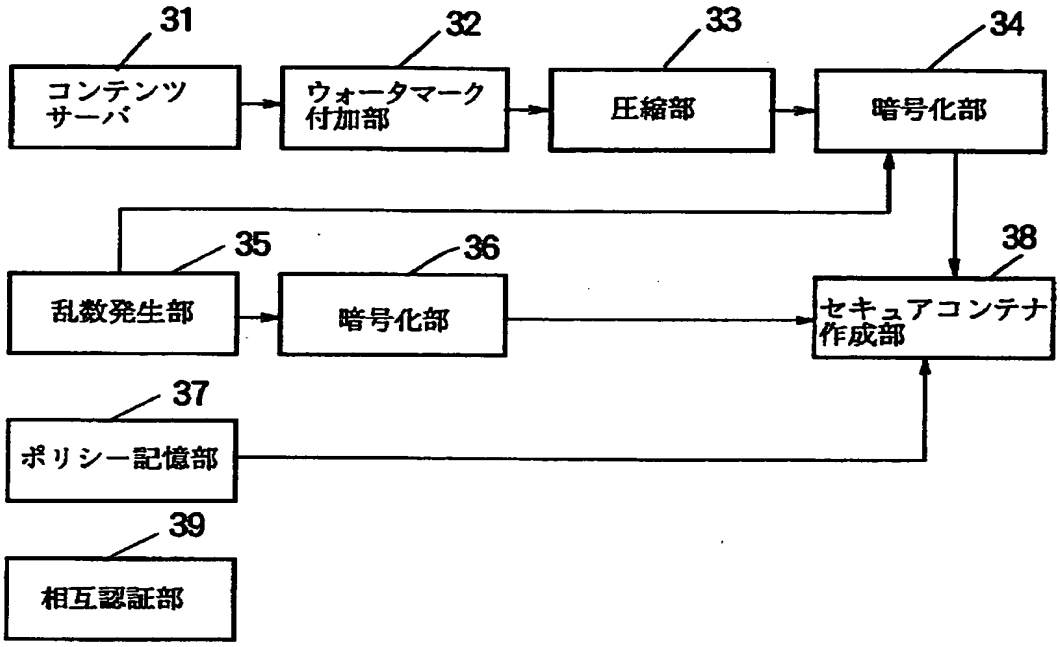
【図６】


コンテンツプロバイダが有する配送用鍵
配送用鍵
ccccccccc
ddddddddd
eeeeeeeee
fffffffff
ggggggggg
hhhhhhhhh
配送用鍵のバージョン
3
4
5
6
7
8
使用可能期間 開始
1998/3/1
1998/4/1
1998/5/1
1998/6/1
1998/7/1
1998/8/1
終了
1998/8/31
1998/4/30
1998/5/31
1998/6/30
1998/7/31
1998/8/31
使用する配送用鍵
配送用鍵を送信
EMDサービスセンタが有する配送用鍵
配送用鍵
aaaaaaaaa
bbbbbbbbb
ccccccccc
ddddddddd
eeeeeeeee
fffffffff
ggggggggg
hhhhhhhhh
配送用鍵のバージョン
1
2
3
4
5
6
7
8
使用可能期間 開始
1998/1/1
1998/2/1
1998/3/1
1998/4/1
1998/5/1
1998/6/1
1998/7/1
1998/8/1
終了
1998/1/31
1998/2/28
1998/3/31
1998/4/30
1998/5/31
1998/6/30
1998/7/31
1998/8/31
使用する配送用鍵
を配送信用鍵
レシーバが有する配送用鍵
配送用鍵
ccccccccc
ddddddddd
eeeeeeeee
配送用鍵のバージョン
8
4
5
使用可能期間 開始
1998/3/1
1998/4/1
1998/5/1
終了
1998/3/31
1998/4/30
1998/5/31
使用する配送用鍵

【図７】


EMD サービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiii 9 1998/9/1 1998/9/30
配送用鍵を送信
使用する配送用鍵
コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiii 9 1998/9/1 1998/9/30
使用する配送用鍵
配送用鍵を配送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵

【図８】



コンテンツプロバイダ 2

【図９】

(A)

コンテンツのID	コンテンツAのID	
コンテンツプロバイダのID	コンテンツプロバイダ2のID	
UCPのID	UCPAのID	
UCPの有効期限	UCPAの有効期限	
利用条件10	ユーザ条件10	200ポイント以上
	機器条件10	条件なし
利用内容11	ID 11	利用内容11のID
	形式11	買い取り再生
	パラメータ11	×××××
	管理移動許可情報11	可
利用内容12	ID 12	利用内容12のID
	形式12	第1世代複製
	パラメータ12	×××××
	管理移動許可情報12	不可
利用内容13	ID 13	利用内容13のID
	形式13	期間制限再生
	パラメータ13	×××××
	管理移動許可情報13	不可
利用内容14	ID 14	利用内容14のID
	形式14	Pay Per Copy 5
	パラメータ14	複製5回
	管理移動許可情報14	不可

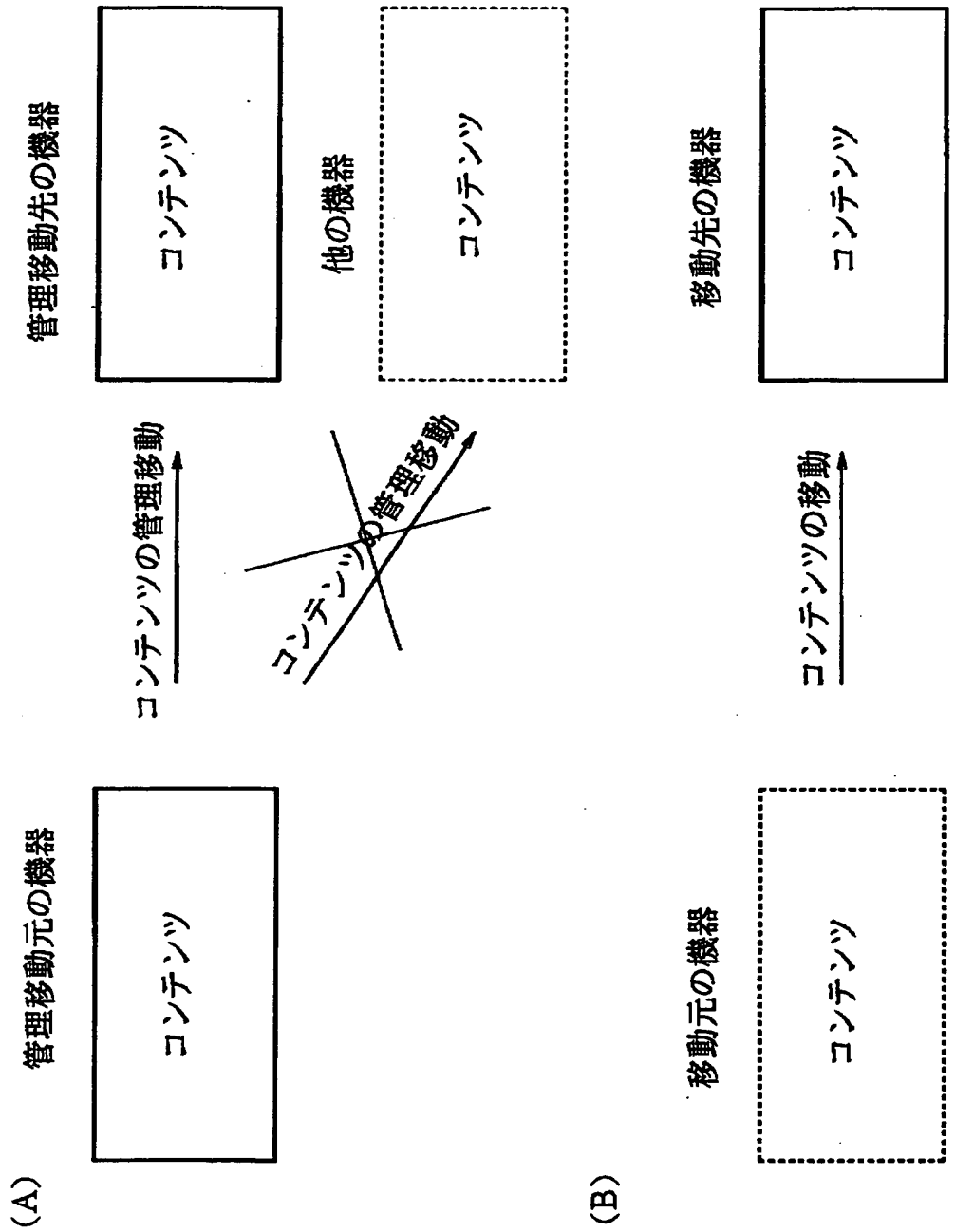
UCPA

(B)

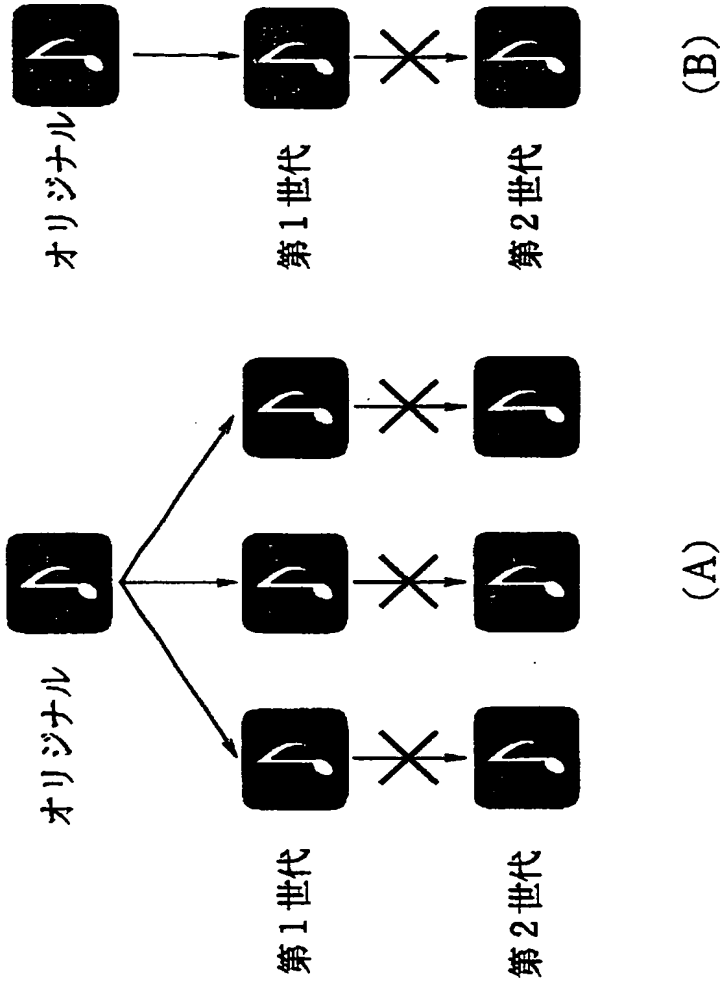
コンテンツのID	コンテンツAのID	
コンテンツプロバイダのID	コンテンツプロバイダ2のID	
UCPのID	UCPBのID	
UCPの有効期限	UCPBの有効期限	
利用条件20	ユーザ条件20	200ポイントより少ない
	機器条件20	条件なし
利用内容21	ID 21	利用内容21のID
	形式21	Pay Per Play 4
	パラメータ21	再生4回
	管理移動許可情報21	不可
利用内容22	ID 22	利用内容22のID
	形式22	Pay Per Copy 2
	パラメータ22	複製2回
	管理移動許可情報22	不可

UCPB

【図１０】


(A)
管理移動元の機器
コンテンツ
コンテンツの管理移動
管理移動先の機器
コンテンツ
他の機器
コンテンツ
コンテンツの管理移動
(B)
移動元の機器
コンテンツ
コンテンツの移動
移動先の機器
コンテンツ

【図１１】



【図１２】

（A）

サービスコード	意　味
0000h	条件なし
0001h 乃至 00FFh	機器に関し条件有り
0100h 乃至 01FFh	性別条件あり
0200h 乃至 02FFh	年令条件あり
0300h 乃至 7FFFh	その他の条件あり
8000h 乃至 FFFFh	利用ポイントに関し条件有り

（B）

コンディションコード	意　味
00h	無条件
01h	＝
02h	≠
03h	＜（より小さい）
04h	＞（より大きい）
05h	≦（以下）
06h	≧（以上）
07h 乃至 FFh	空き

【図１３】

（A）

ユーザ条件 10	サービスコード	バリューコード	コンディションコード
	80××h	0000C8h	06h
機器条件 10	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

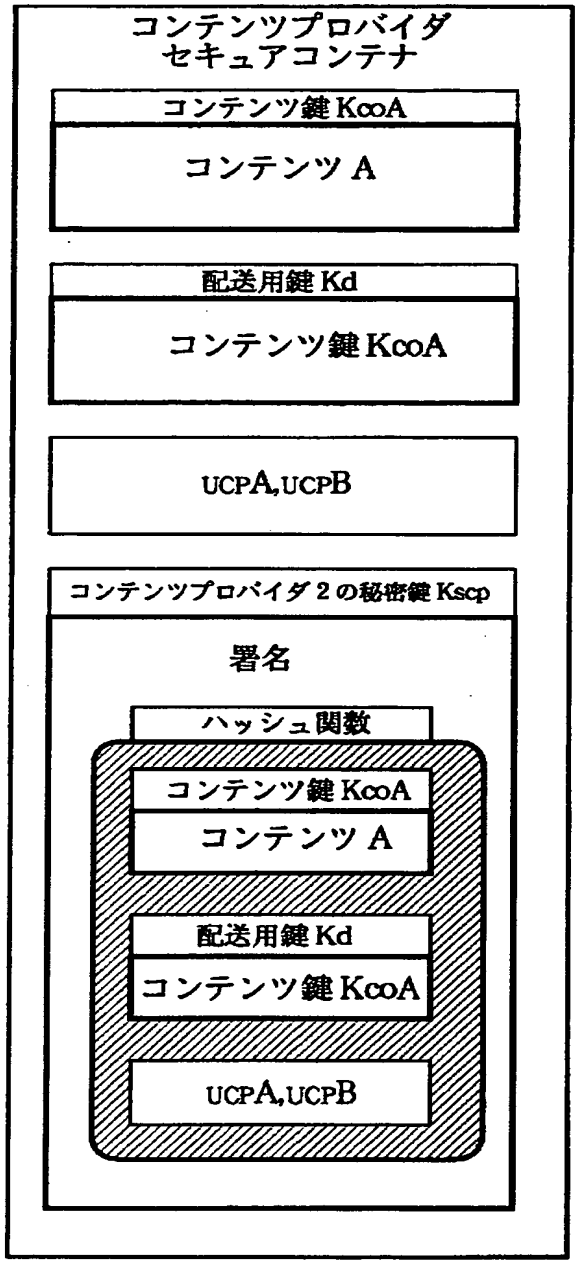
UCPA の利用条件 10

（B）

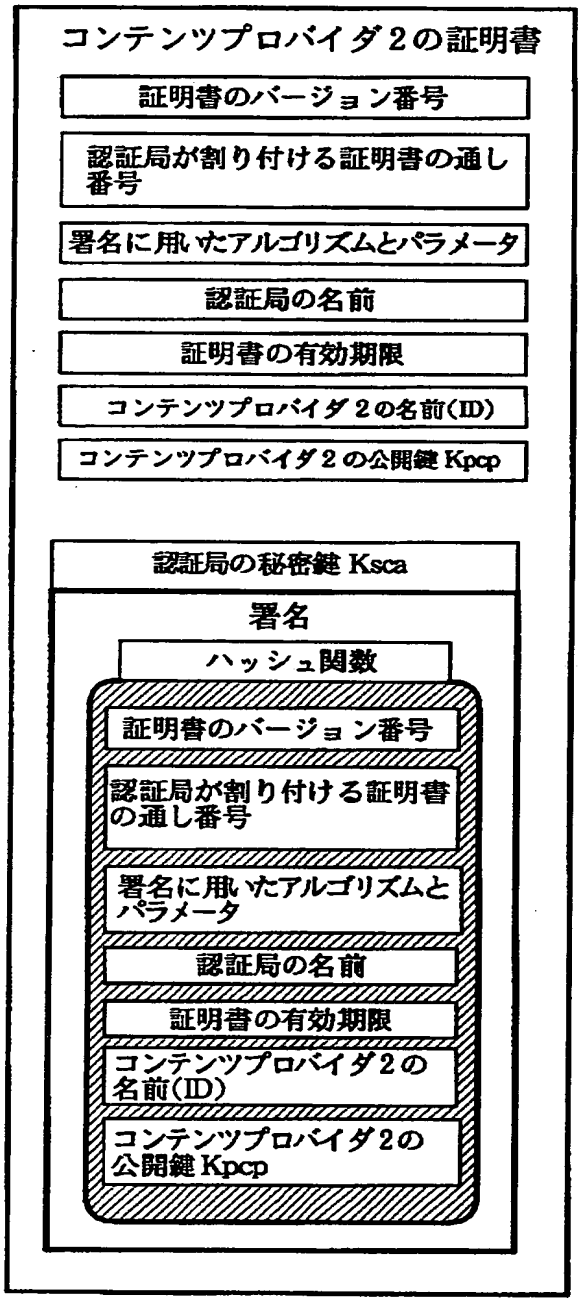
ユーザ条件 20	サービスコード	バリューコード	コンディションコード
	80××h	0000C8h	03h
機器条件 20	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

UCPB の利用条件 20

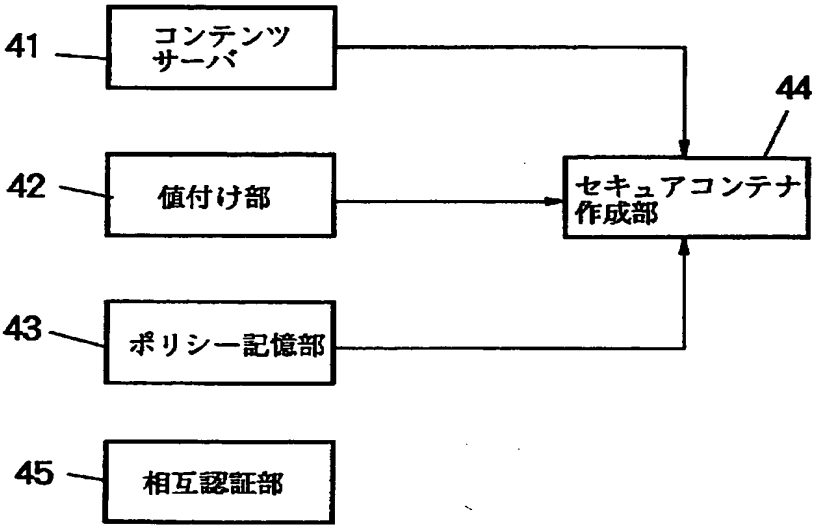
【図１４】


コンテンツプロバイダ
セキュアコンテナ
コンテンツ鍵 KcoA
コンテンツ A
配送用鍵 Kd
コンテンツ鍵 KcoA
UCPA,UCPB
コンテンツプロバイダ２の秘密鍵 Kscp
署名
ハッシュ関数
コンテンツ鍵 KcoA
コンテンツ A
配送用鍵 Kd
コンテンツ鍵 KcoA
UCPA,UCPB

【図１５】


コンテンツプロバイダ２の証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
コンテンツプロバイダ２の名前(ID)
コンテンツプロバイダ２の公開鍵 Kpcp
認証局の秘密鍵 Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
コンテンツプロバイダ２の名前(ID)
コンテンツプロバイダ２の公開鍵 Kpcp

【図１６】


41
コンテンツ
サーバ
44
42
値付け部
セキュアコンテナ
作成部
43
ポリシー記憶部
45
相互認証部
サービスプロバイダ 3

【図１７】

コンテンツのID	コンテンツAのID		
コンテンツプロバイダのID	コンテンツプロバイダ2のID		
UCPのID	UCPAのID		
UCPの有効期限	UCPAの有効期限		
サービスプロバイダのID	サービスプロバイダ3のID		
PTのID	PTA-1のID		
PTの有効期限	PTA-1の有効期限		
価格条件10	ユーザ条件10	男性	
	機器条件10	条件なし	
価格内容11	2000円		
価格内容12	600円		
価格内容13	100円		
価格内容14	300円		

PTA-1

コンテンツのID	コンテンツAのID		
コンテンツプロバイダのID	コンテンツプロバイダ2のID		
UCPのID	UCPAのID		
UCPの有効期限	UCPAの有効期限		
サービスプロバイダのID	サービスプロバイダ3のID		
PTのID	PTA-2のID		
PTの有効期限	PTA-2の有効期限		
価格条件20	ユーザ条件20	女性	
	機器条件20	条件なし	
価格内容21	1000円		
価格内容22	900円		
価格内容23	50円		
価格内容24	150円		

PTA-2

【図１８】

（A）

ユーザ条件 10	サービスコード	バリューコード	コンディションコード
	01××h	000000h	01h
機器条件 10	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-1 の価格条件 10

（B）

ユーザ条件 20	サービスコード	バリューコード	コンディションコード
	01××h	000001h	01h
機器条件 20	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-2 の価格条件 20

【図１９】

コンテンツのID	コンテンツAのID		
コンテンツプロバイダのID	コンテンツプロバイダ2のID		
UCPのID	UCPBのID		
サービスプロバイダのID	サービスプロバイダ3のID		
PTのID	PTB-1のID		
PTの有効期限	PTB-1の有効期限		
価格条件30	ユーザ条件30	条件なし	
	機器条件30	従機器	
価格内容31	100円		
価格内容32	300円		

PTB-1

(A)

コンテンツのID	コンテンツAのID		
コンテンツプロバイダのID	コンテンツプロバイダ2のID		
UCPのID	UCPBのID		
サービスプロバイダのID	サービスプロバイダ3のID		
PTのID	PTB-2のID		
PTの有効期限	PTB-2の有効期限		
価格条件40	ユーザ条件40	条件なし	
	機器条件40	主機器	
価格内容41	50円		
価格内容42	150円		

PTB-2

(B)

【図２０】

（A）

ユーザ条件 30	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 30	サービスコード	バリューコード	コンディションコード
	00××h	000064h	03h

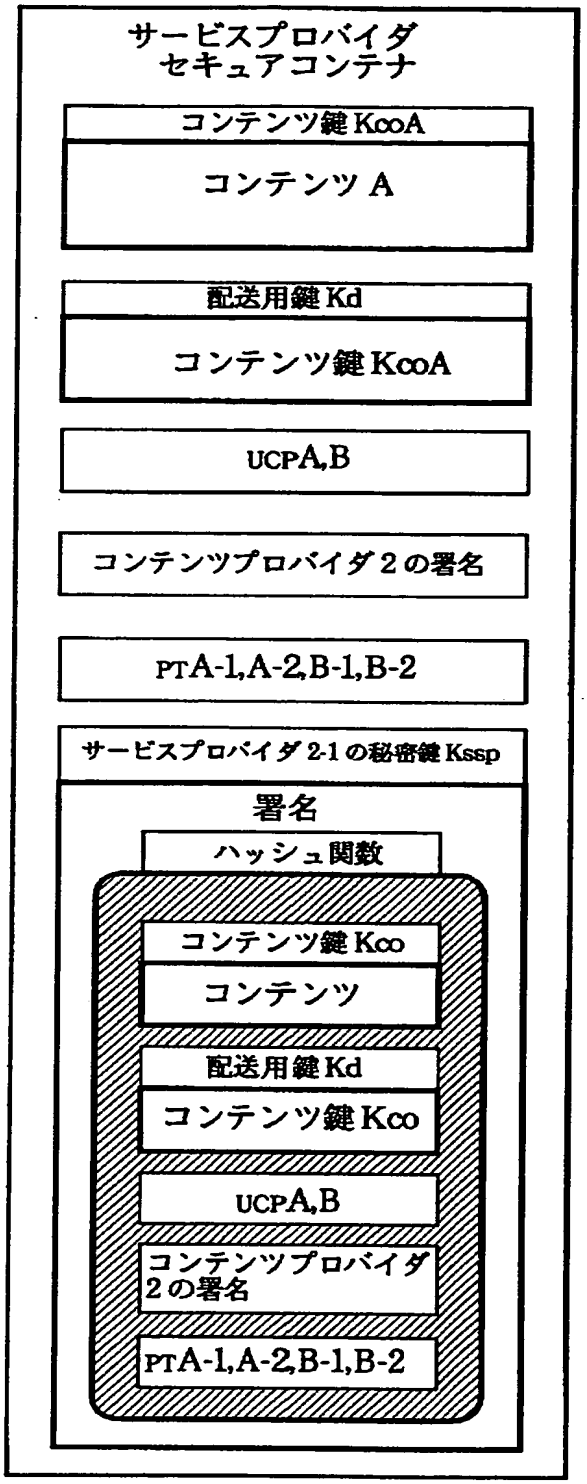
PTB-1 の価格条件 30

（B）

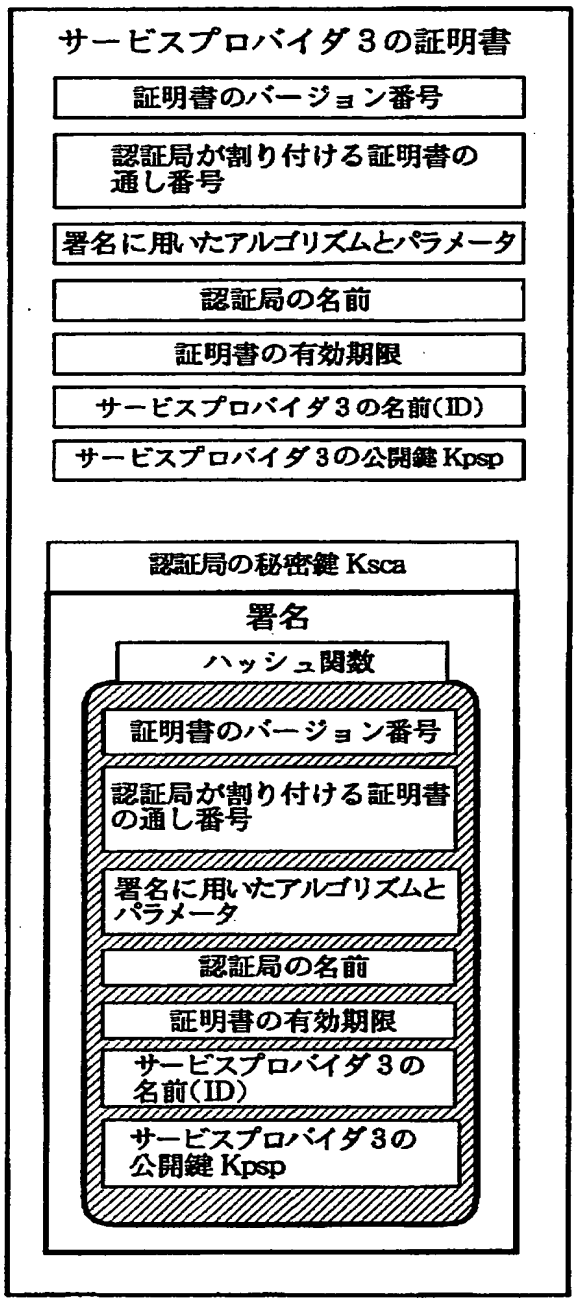
ユーザ条件 40	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 40	サービスコード	バリューコード	コンディションコード
	00××h	000064h	06h

PTB-2 の価格条件 40

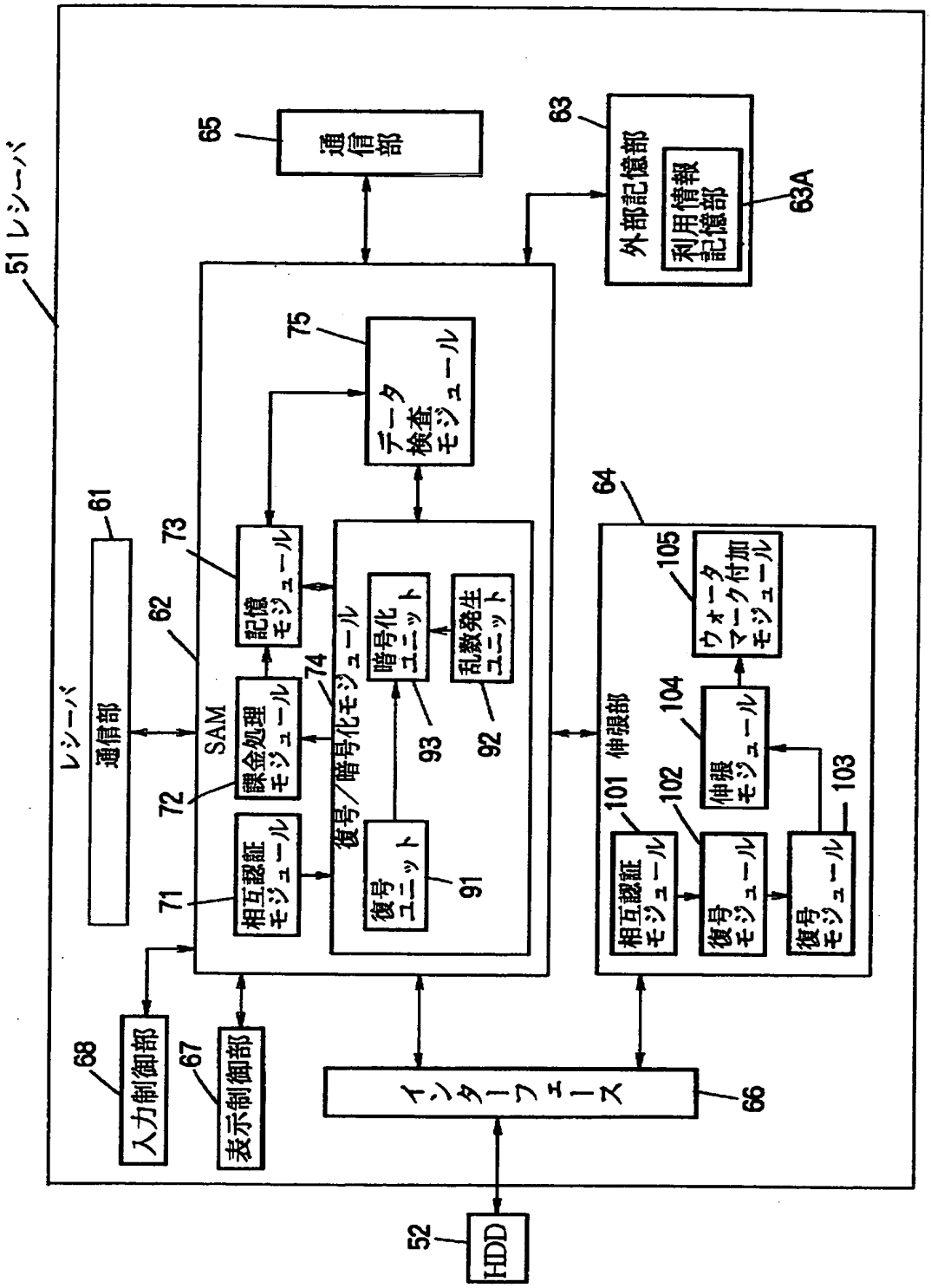
【図２１】


サービスプロバイダ
セキュアコンテナ
コンテンツ鍵KcoA
コンテンツA
配送用鍵Kd
コンテンツ鍵KcoA
UCPA,B
コンテンツプロバイダ２の署名
PTA-1,A-2,B-1,B-2
サービスプロバイダ2-1の秘密鍵Kssp
署名
ハッシュ関数
コンテンツ鍵Kco
コンテンツ
配送用鍵Kd
コンテンツ鍵Kco
UCPA,B
コンテンツプロバイダ2の署名
PTA-1,A-2,B-1,B-2

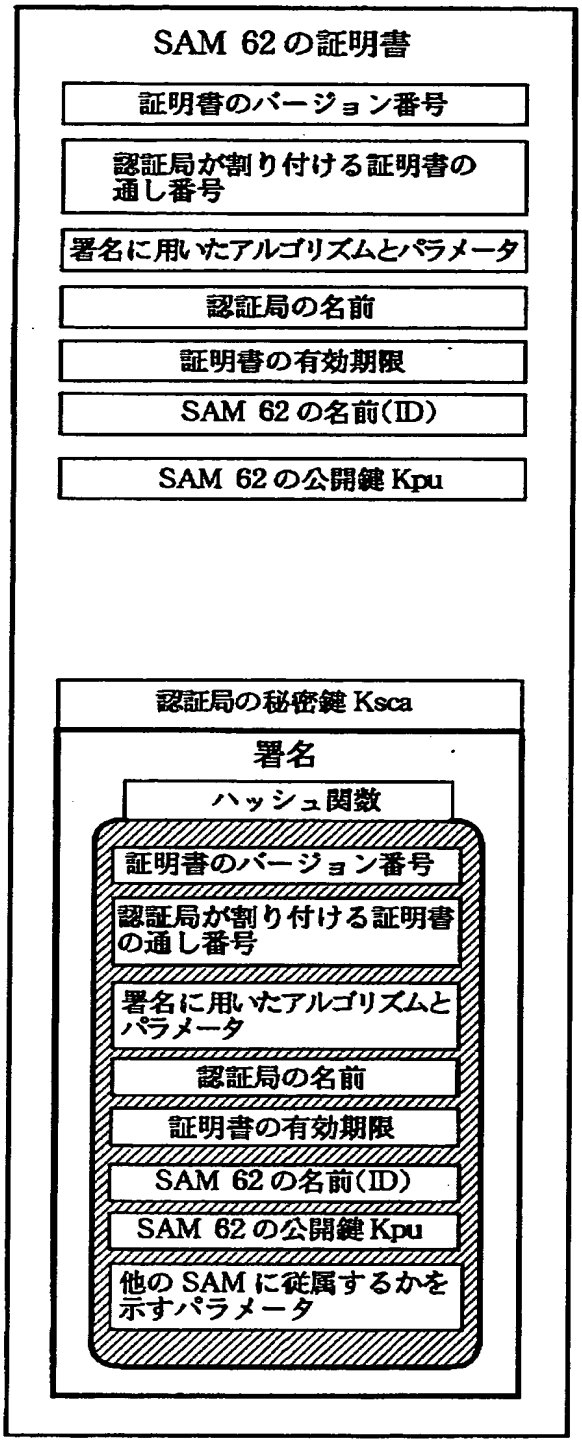
【図２２】


サービスプロバイダ３の証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
サービスプロバイダ３の名前(ID)
サービスプロバイダ３の公開鍵 Kpsp
認証局の秘密鍵 Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
サービスプロバイダ３の名前(ID)
サービスプロバイダ３の公開鍵 Kpsp

【図２３】


51 レシーバ
65
通信部
63
外部記憶部
利用情報記憶部
63A
75
データ検査モジュール
64
61
73
記憶モジュール
105
ウォータマーク付加モジュール
62
レシーバ通信部
SAM
課金処理モジュール
74
暗号化モジュール
暗号化ユニット
乱数発生ユニット
104
伸張モジュール
72
93
92
伸張部
101
102
103
71
相互認証モジュール
復号ユニット
91
相互認証モジュール
復号モジュール
復号モジュール
68
入力制御部
67
表示制御部
インターフェース
66
52
HDD

【図２４】

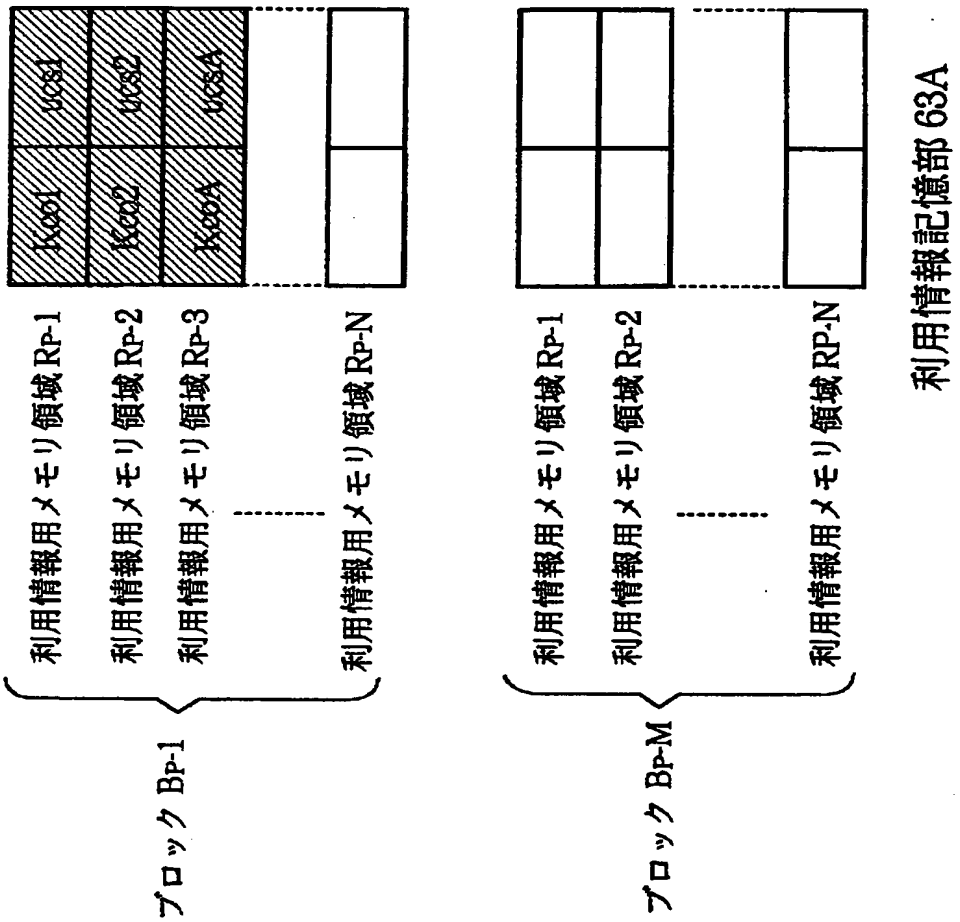

SAM 62の証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
SAM 62の名前(ID)
SAM 62の公開鍵Kpu
認証局の秘密鍵Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
SAM 62の名前(ID)
SAM 62の公開鍵Kpu
他のSAMに従属するかを示すパラメータ

【図２５】

コンテンツのID		コンテンツAのID
コンテンツプロバイダのID		コンテンツプロバイダ2のID
UCPのID		UCPAのID
UCPの有効期限		UCPAの有効期限
サービスプロバイダのID		サービスプロバイダ3のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		UCSAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容11のID
	形式	買い取り再生
	パラメータ	×××
	管理移動状態情報	管理移動元：SAM62のID、管理移動先：SAM62のID
利用履歴		×××

UCSA

【図２６】

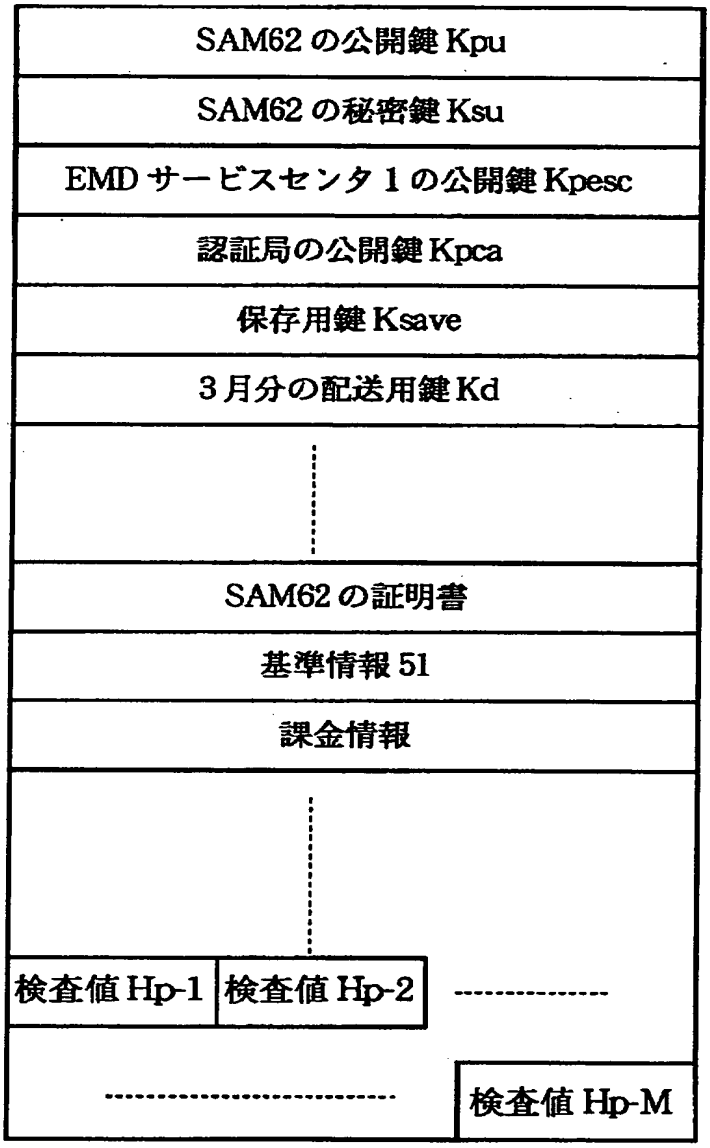

利用情報記憶部 63A
ブロック BP-1
利用情報用メモリ領域 RP-1
利用情報用メモリ領域 RP-2
利用情報用メモリ領域 RP-3
利用情報用メモリ領域 RP-N
Kos1
Kos2
KosA
ucs1
ucs2
ucsA
ブロック BP-M
利用情報用メモリ領域 RP-1
利用情報用メモリ領域 RP-2
利用情報用メモリ領域 RP-N

【図２７】

コンテンツのID		コンテンツAのID
コンテンツプロバイダのID		コンテンツプロバイダ2のID
UCPのID		UCPAのID
UCPの有効期限		UCPAの有効期限
サービスプロバイダのID		サービスプロバイダ3のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		UCSAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容11のID
	形式	買い取り再生
	パラメータ	×××
	管理移動状態情報	管理移動元：SAM62のID、管理移動先：SAM62のID
課金履歴		×××

課金情報A

【図２８】


SAM62の公開鍵Kpu
SAM62の秘密鍵Ksu
EMDサービスセンタ1の公開鍵Kpesc
認証局の公開鍵Kpca
保存用鍵Ksave
3月分の配送用鍵Kd
SAM62の証明書
基準情報51
課金情報
検査値Hp-1
検査値Hp-2
検査値Hp-M

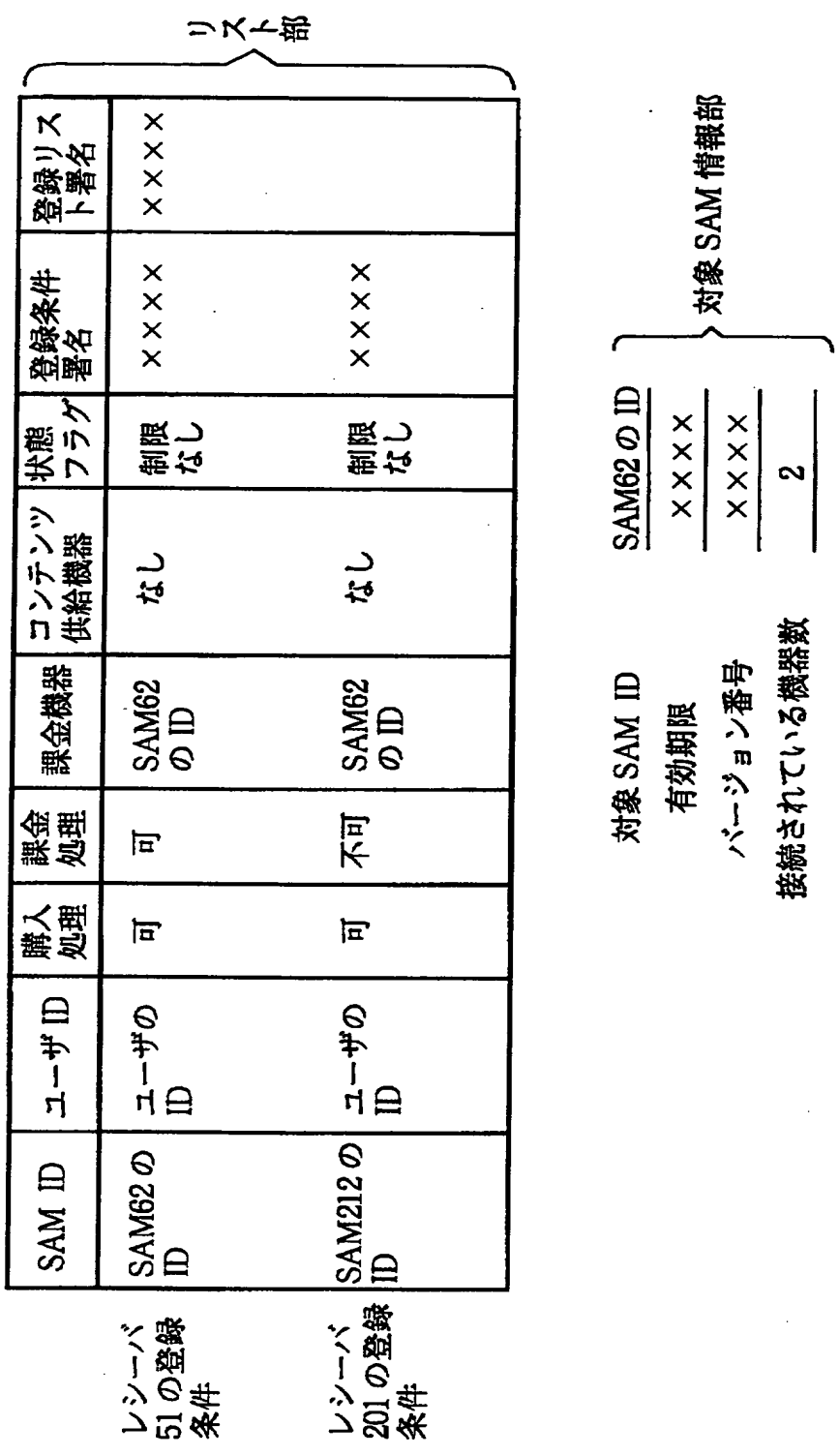
【図２９】

SAM の ID		SAM62 の ID
機器番号		レシーバ 51 の機器番号（100 番）
決済 ID		ユーザの決済 ID
課金の上限額		正式登録時の課金の上限額
決済ユーザ情報	氏名	ユーザの氏名
	住所	ユーザの住所
	電話番号	ユーザの電話番号
	決済機関情報	ユーザの決済機関情報
	生年月日	ユーザの生年月日
	年齢	ユーザの年齢（21 才）
	性別	ユーザの性別（男）
	ユーザの ID	ユーザの ID
	パスワード	ユーザのパスワード

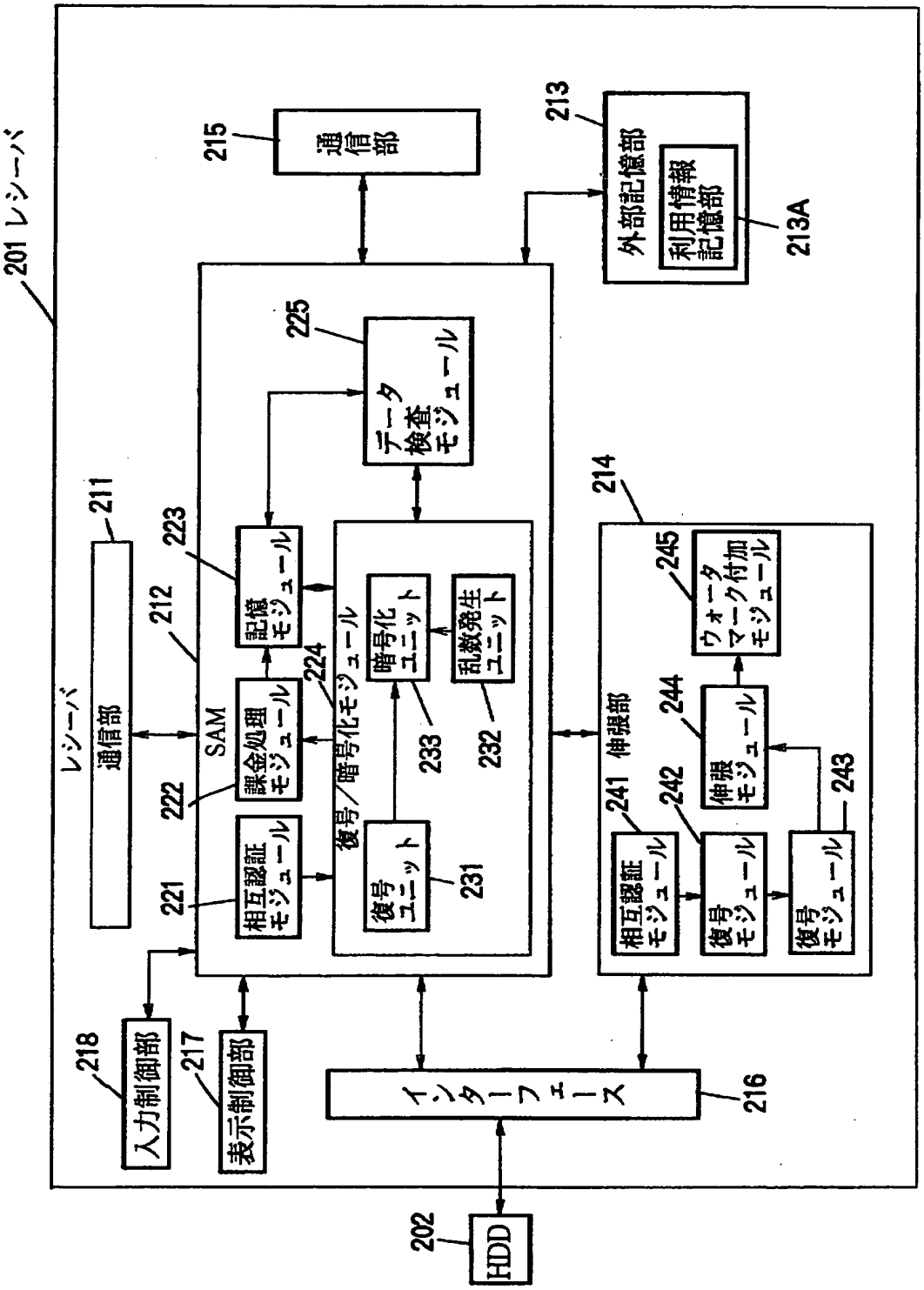
利用ポイント情報	レシーバ 51 の利用ポイント情報

基準情報 51

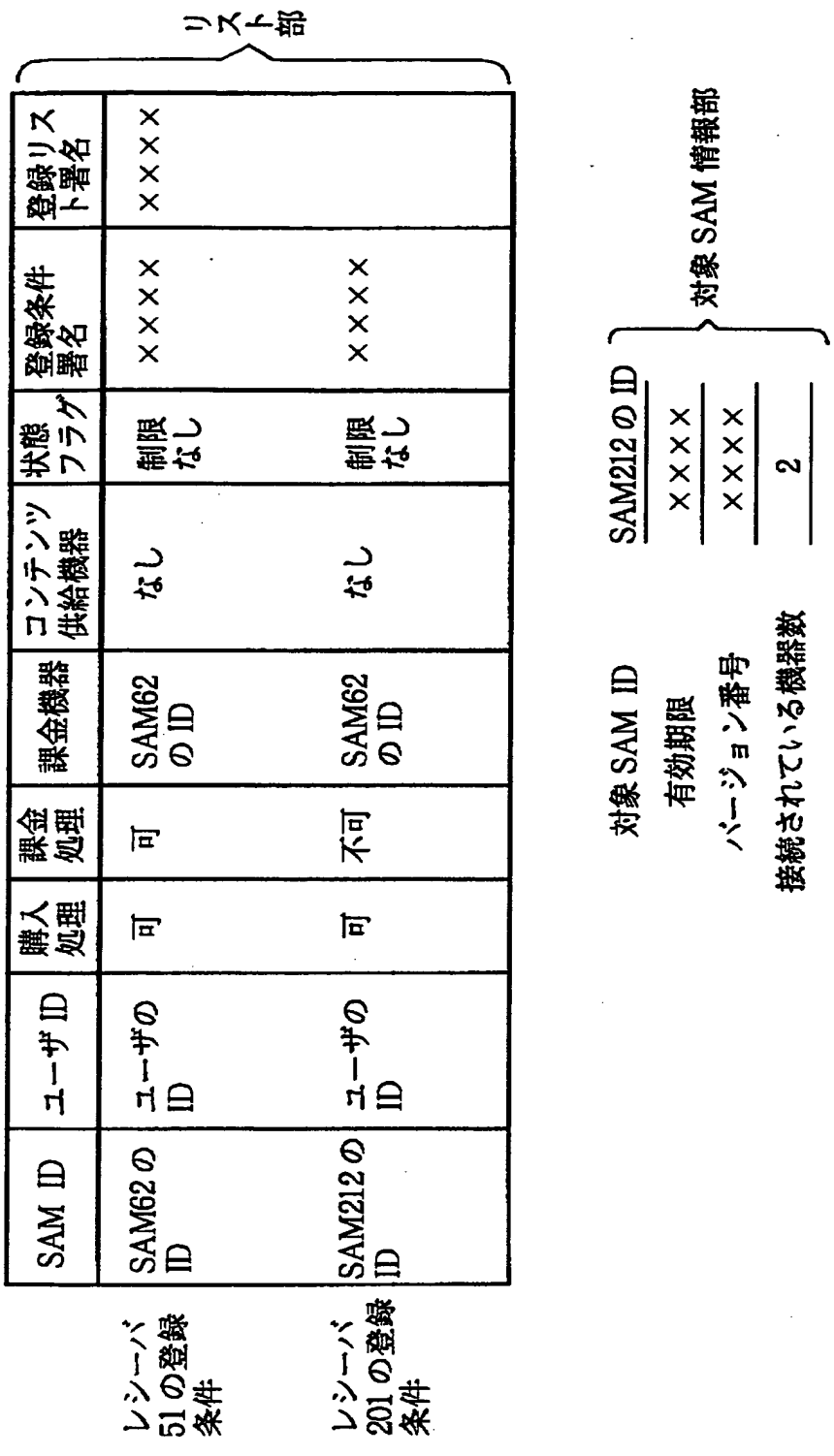
【図３０】


リスト部
SAM ID
ユーザ ID
購入処理
課金処理
課金機器
コンテンツ供給機器
状態フラグ
登録条件署名
登録リスト署名
SAM62のID
ユーザのID
可
可
SAM62のID
なし
制限なし
××××
××××
SAM212のID
ユーザのID
可
不可
SAM62のID
なし
制限なし
××××
レシーバ51の登録条件
レシーバ201の登録条件
対象SAM ID
有効期限
バージョン番号
接続されている機器数
SAM62のID
××××
××××
2
対象SAM情報部
レシーバ51の登録リスト

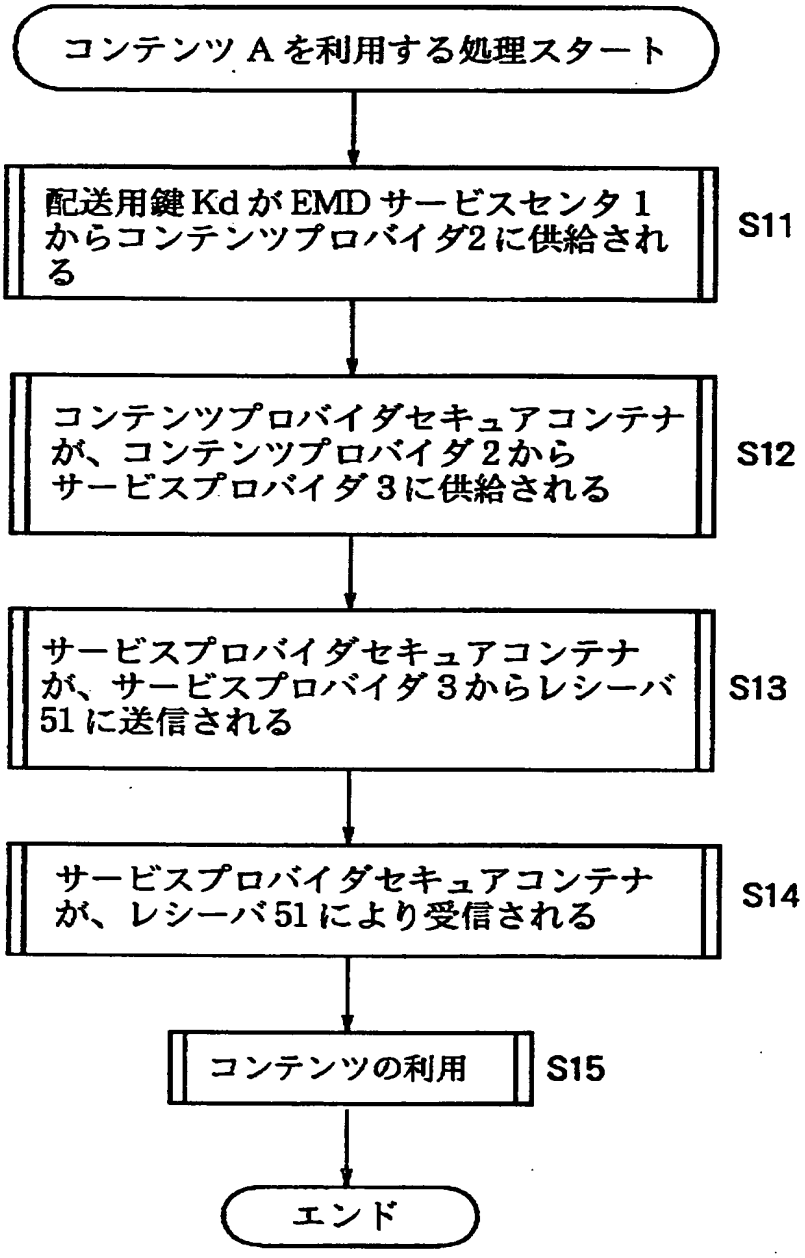
【図３１】


201 レシーバ
215 通信部
213 外部記憶部
利用情報記憶部
213A
225 データ検査モジュール
214
211
223 記憶モジュール
212
224
暗号化ユニット
乱数発生ユニット
245 ウォータマーク付加モジュール
レシーバ通信部
SAM
222 課金処理モジュール
復号／暗号化モジュール
233
232
244 伸張モジュール
241 伸張部
242
243
221 相互認証モジュール
復号ユニット
231
相互認証モジュール
復号モジュール
復号モジュール
218 入力制御部
217 表示制御部
インターフェース
216
202 HDD

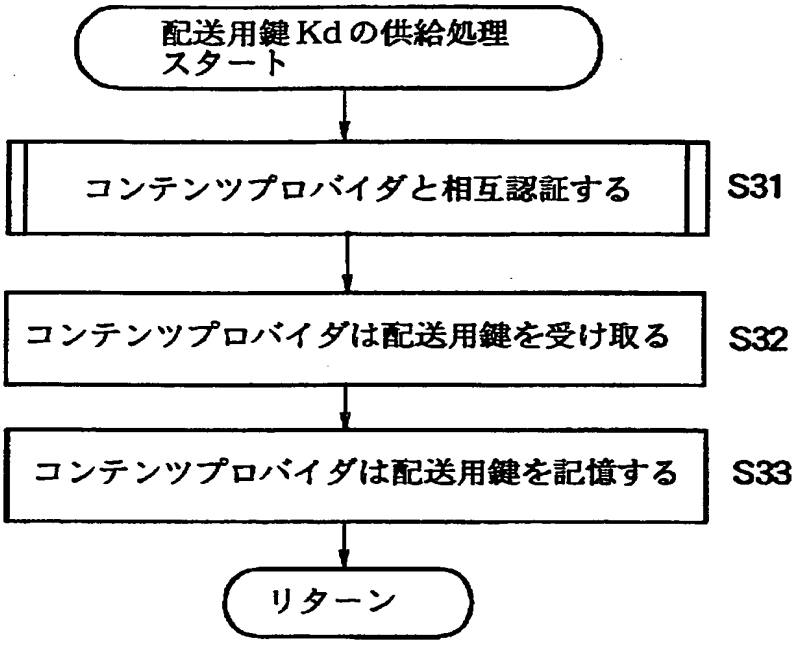
【図３２】


リスト部
SAM ID
ユーザ ID
購入処理
課金処理
課金機器
コンテンツ供給機器
状態フラグ
登録条件署名
登録リスト署名
SAM62のID
ユーザのID
可
可
SAM62のID
なし
制限なし
××××
××××
SAM212のID
ユーザのID
可
不可
SAM62のID
なし
制限なし
××××
××××
レシーバ51の登録条件
レシーバ201の登録条件
対象SAM ID
SAM212のID
有効期限
××××
バージョン番号
××××
接続されている機器数
2
対象SAM情報部
レシーバ201の登録リスト

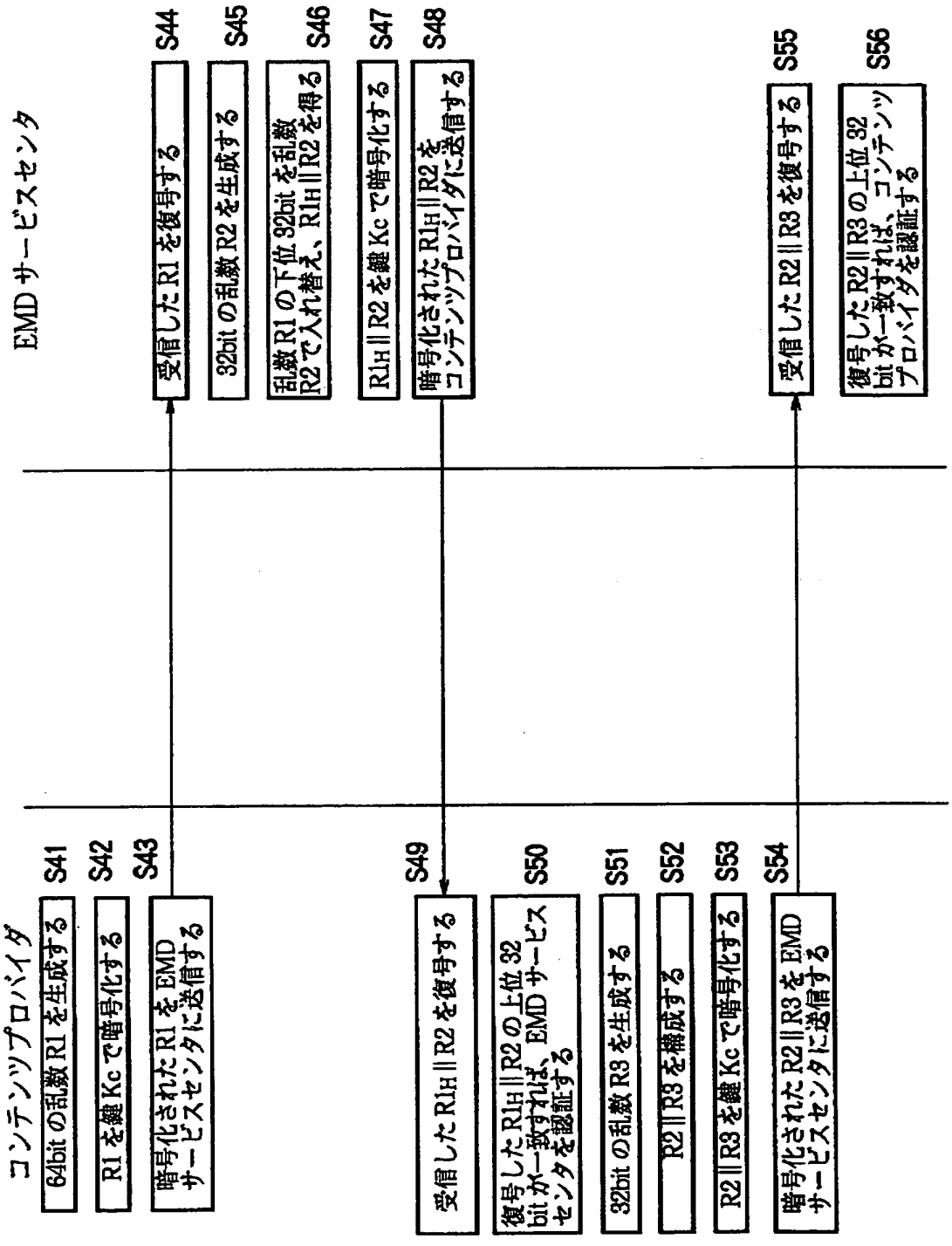
【図３３】


コンテンツＡを利用する処理スタート
配送用鍵KdがEMDサービスセンタ1からコンテンツプロバイダ2に供給される
S11
コンテンツプロバイダセキュアコンテナが、コンテンツプロバイダ2からサービスプロバイダ3に供給される
S12
サービスプロバイダセキュアコンテナが、サービスプロバイダ3からレシーバ51に送信される
S13
サービスプロバイダセキュアコンテナが、レシーバ51により受信される
S14
コンテンツの利用
S15
エンド

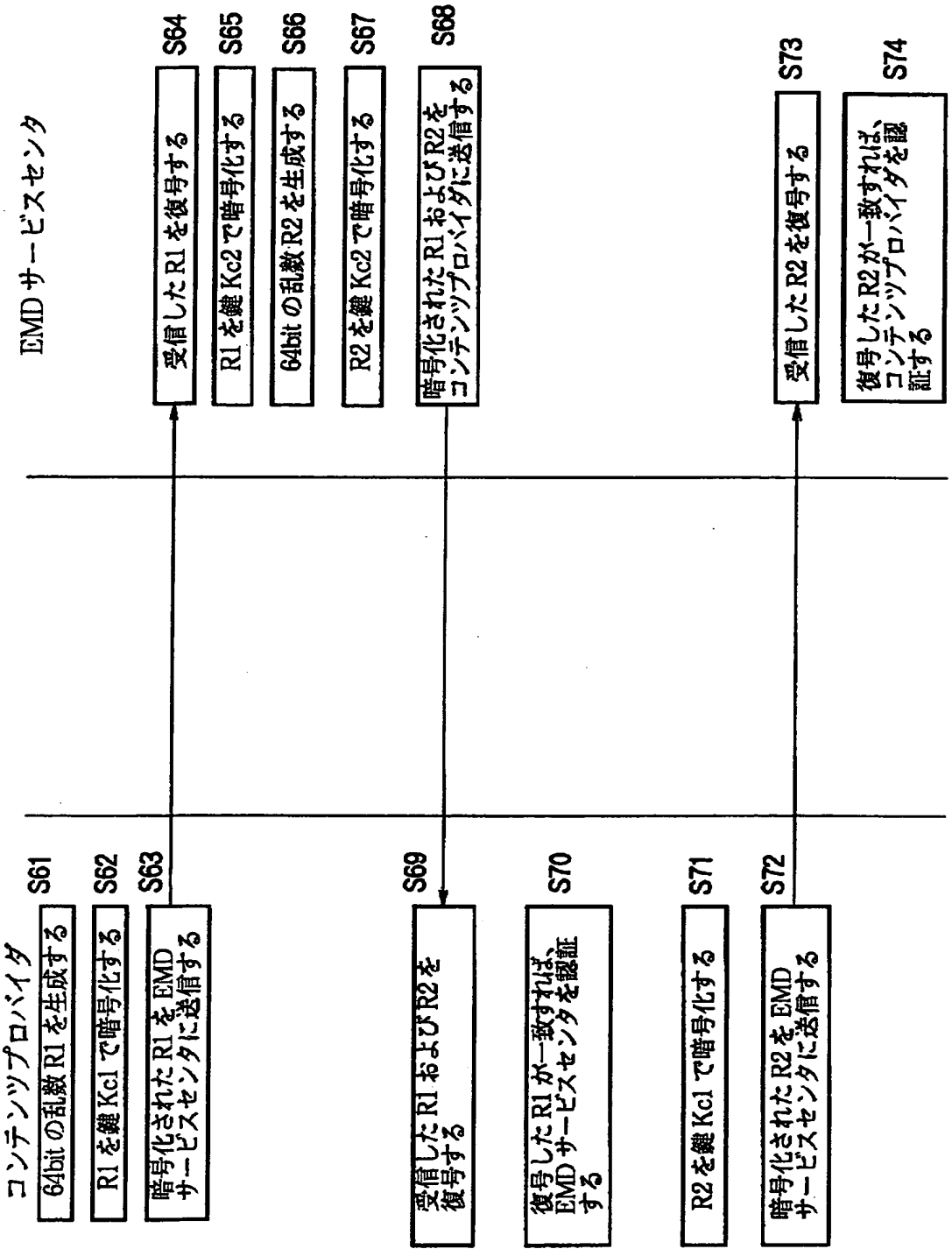
【図３４】


配送用鍵Kdの供給処理
スタート
コンテンツプロバイダと相互認証する
S31
コンテンツプロバイダは配送用鍵を受け取る
S32
コンテンツプロバイダは配送用鍵を記憶する
S33
リターン

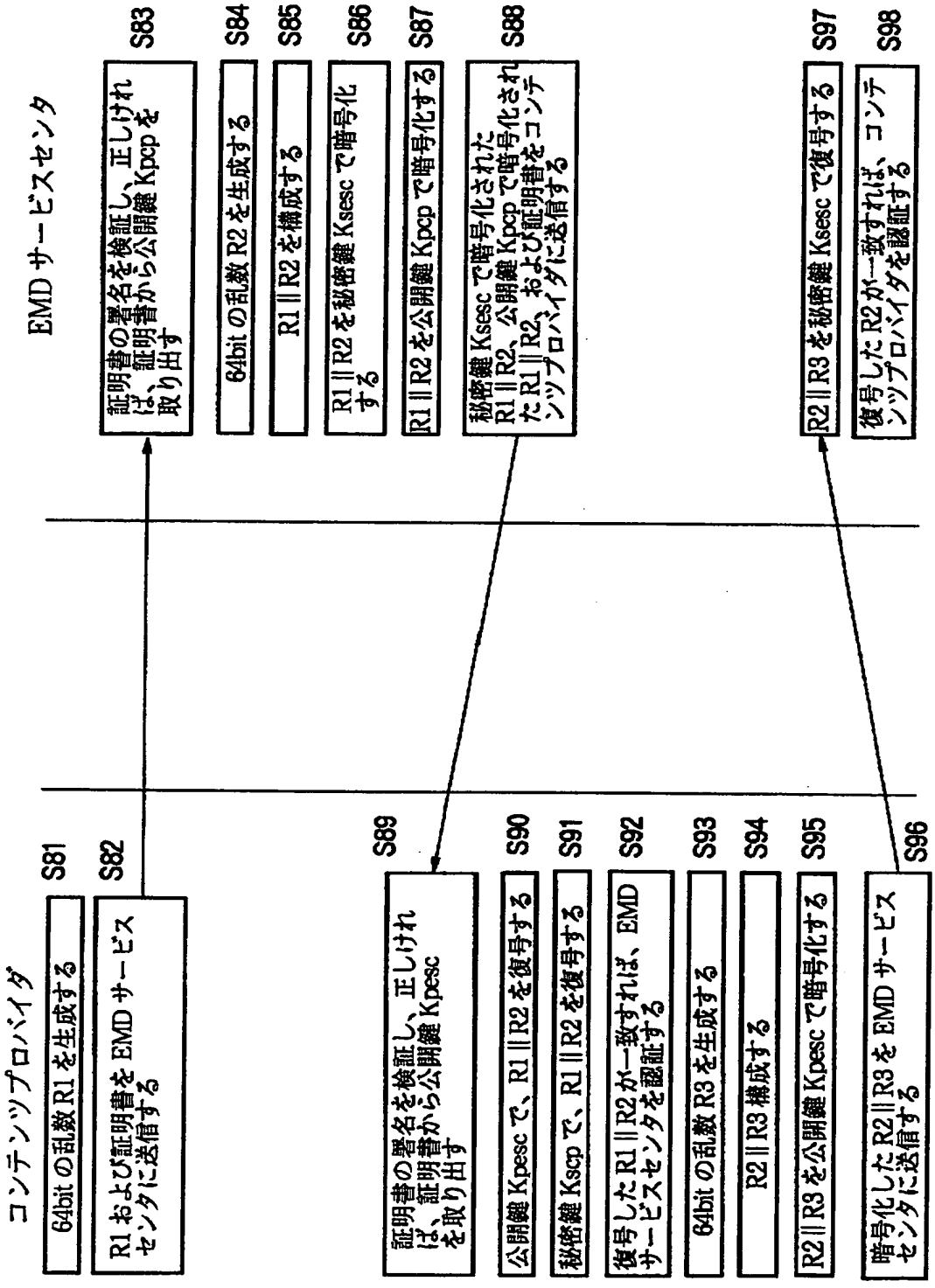
【図３５】


コンテンツプロバイダ
EMDサービスセンタ
S41
64bitの乱数R1を生成する
S42
R1を鍵Kcで暗号化する
S43
暗号化されたR1をEMDサービスセンタに送信する
S44
受信したR1を復号する
S45
32bitの乱数R2を生成する
S46
乱数R1の下位32bitを乱数R2で入れ替え、R1H||R2を得る
S47
R1H||R2を鍵Kcで暗号化する
S48
暗号化されたR1H||R2をコンテンツプロバイダに送信する
S49
受信したR1H||R2を復号する
S50
復号したR1H||R2の上位32bitが一致すれば、EMDサービスセンタを認証する
S51
32bitの乱数R3を生成する
S52
R2||R3を構成する
S53
R2||R3を鍵Kcで暗号化する
S54
暗号化されたR2||R3をEMDサービスセンタに送信する
S55
受信したR2||R3を復号する
S56
復号したR2||R3の上位32bitが一致すれば、コンテンツプロバイダを認証する

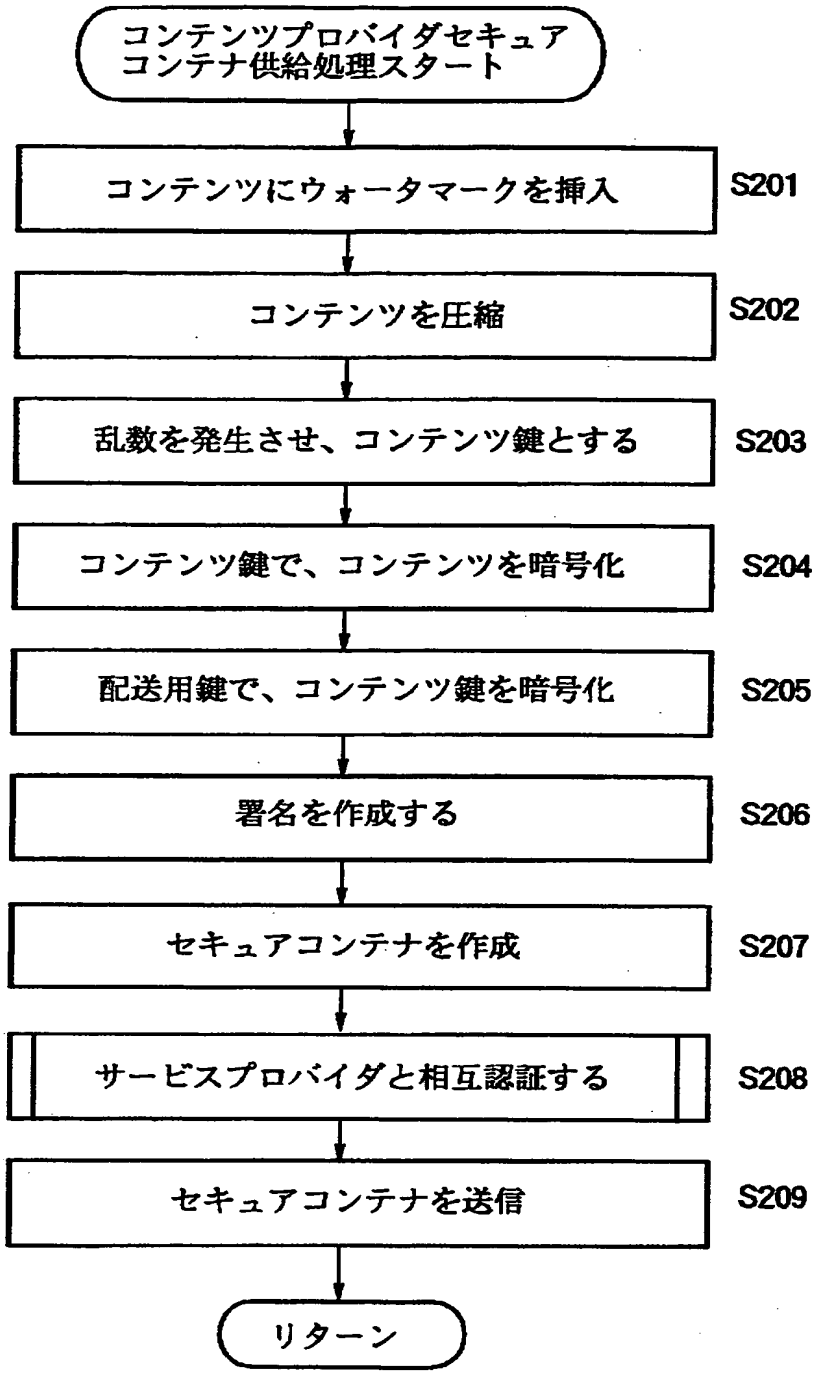
【図３６】


コンテンツプロバイダ
EMDサービスセンタ
S61
64bitの乱数R1を生成する
S62
R1を鍵Kc1で暗号化する
S63
暗号化されたR1をEMDサービスセンタに送信する
S64
受信したR1を復号する
S65
R1を鍵Kc2で暗号化する
S66
64bitの乱数R2を生成する
S67
R2を鍵Kc2で暗号化する
S68
暗号化されたR1およびR2をコンテンツプロバイダに送信する
S69
受信したR1およびR2を復号する
S70
復号したR1が一致すれば、EMDサービスセンタを認証する
S71
R2を鍵Kc1で暗号化する
S72
暗号化されたR2をEMDサービスセンタに送信する
S73
受信したR2を復号する
S74
復号したR2が一致すれば、コンテンツプロバイダを認証する

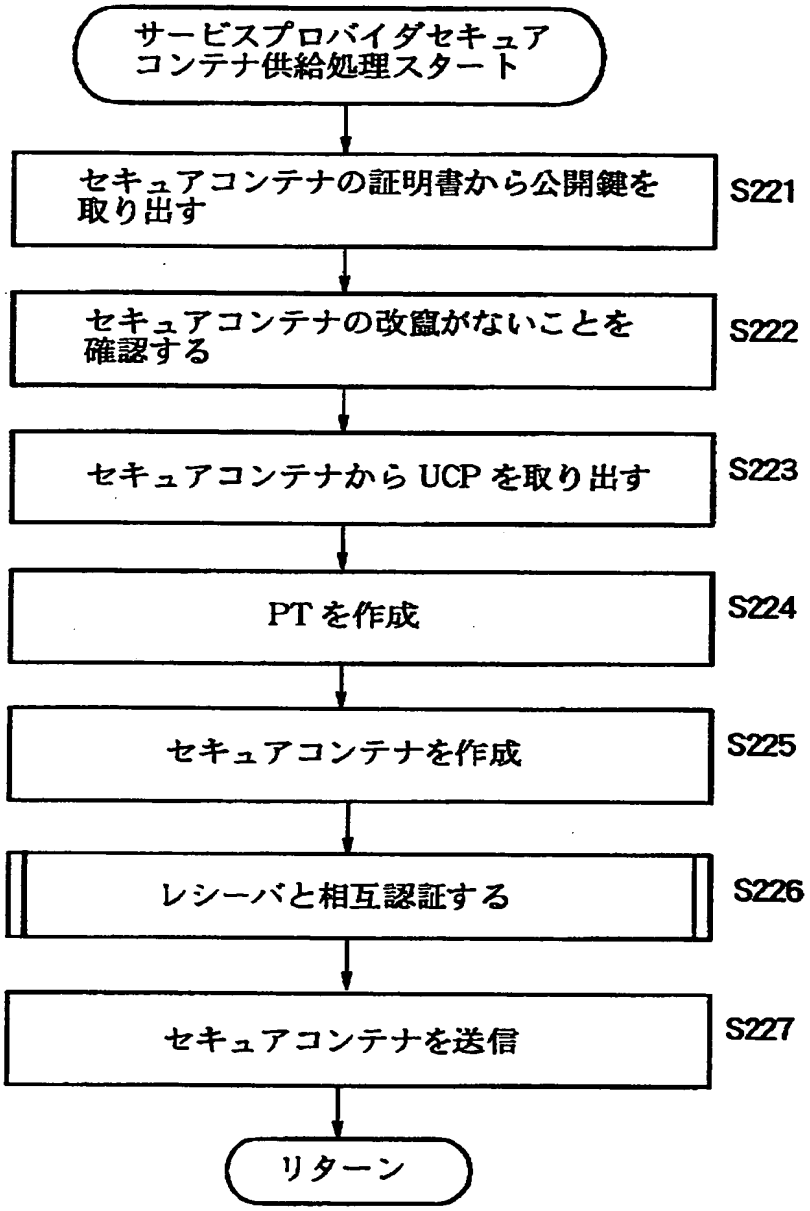
【図３７】


コンテンツプロバイダ
EMD サービスセンタ
S81
64bit の乱数 R1 を生成する
S82
R1 および証明書を EMD サービスセンタに送信する
S83
証明書の署名を検証し、正しければ、証明書から公開鍵 Kpcp を取り出す
S84
64bit の乱数 R2 を生成する
S85
R1 ‖ R2 を構成する
S86
R1 ‖ R2 を秘密鍵 Ksesc で暗号化する
S87
R1 ‖ R2 を公開鍵 Kpcp で暗号化する
S88
秘密鍵 Ksesc で暗号化された R1 ‖ R2、公開鍵 Kpcp で暗号化された R1 ‖ R2、および証明書をコンテンツプロバイダに送信する
S89
証明書の署名を検証し、正しければ、証明書から公開鍵 Kpesc を取り出す
S90
公開鍵 Kpesc で、R1 ‖ R2 を復号する
S91
秘密鍵 Kscp で、R1 ‖ R2 を復号する
S92
復号した R1 ‖ R2 が一致すれば、EMD サービスセンタを認証する
S93
64bit の乱数 R3 を生成する
S94
R2 ‖ R3 構成する
S95
R2 ‖ R3 を公開鍵 Kpesc で暗号化する
S96
暗号化した R2 ‖ R3 を EMD サービスセンタに送信する
S97
R2 ‖ R3 を秘密鍵 Ksesc で復号する
S98
復号した R2 が一致すれば、コンテンツプロバイダを認証する

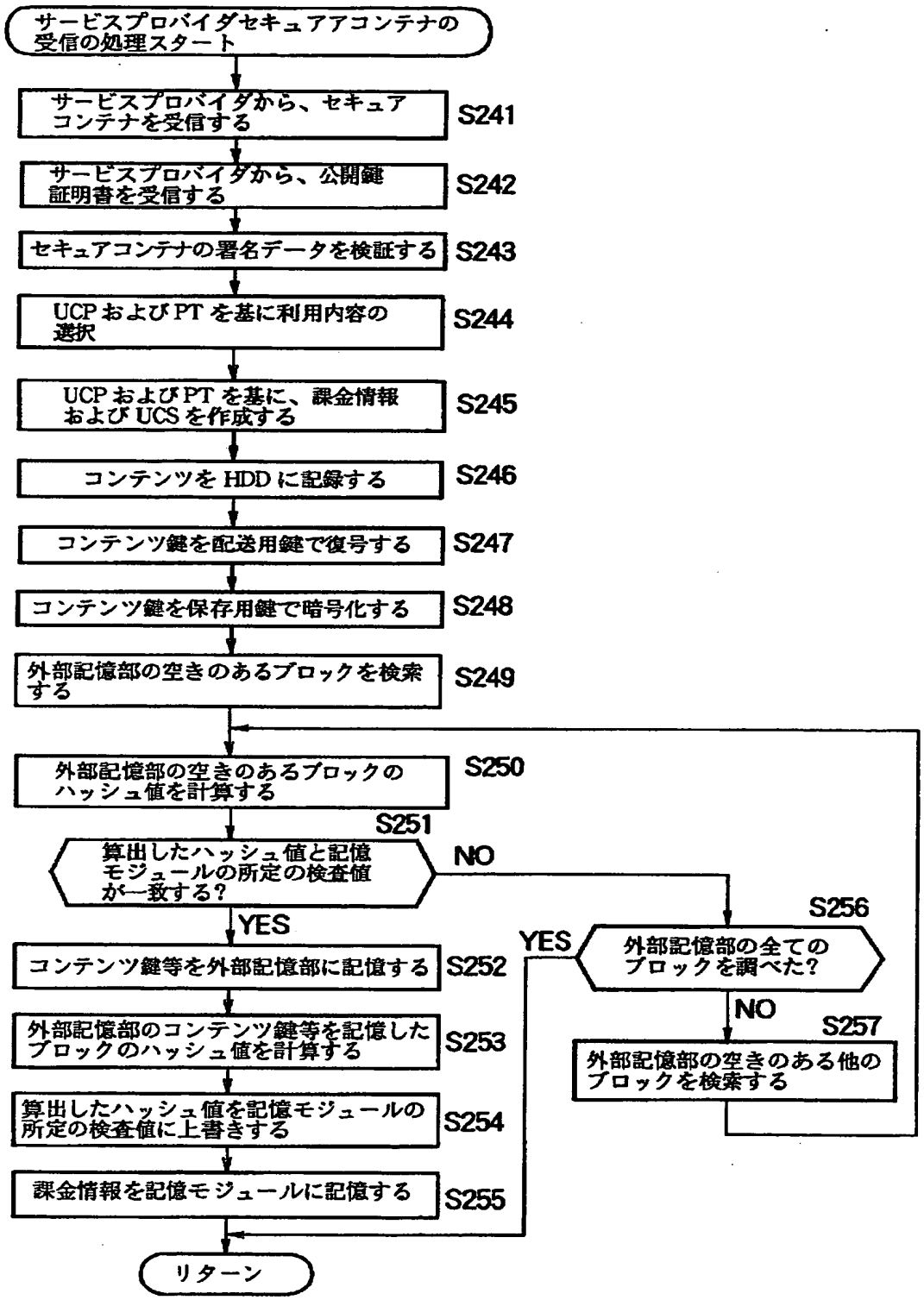
【図３８】


コンテンツプロバイダセキュア
コンテナ供給処理スタート
コンテンツにウォータマークを挿入
S201
コンテンツを圧縮
S202
乱数を発生させ、コンテンツ鍵とする
S203
コンテンツ鍵で、コンテンツを暗号化
S204
配送用鍵で、コンテンツ鍵を暗号化
S205
署名を作成する
S206
セキュアコンテナを作成
S207
サービスプロバイダと相互認証する
S208
セキュアコンテナを送信
S209
リターン

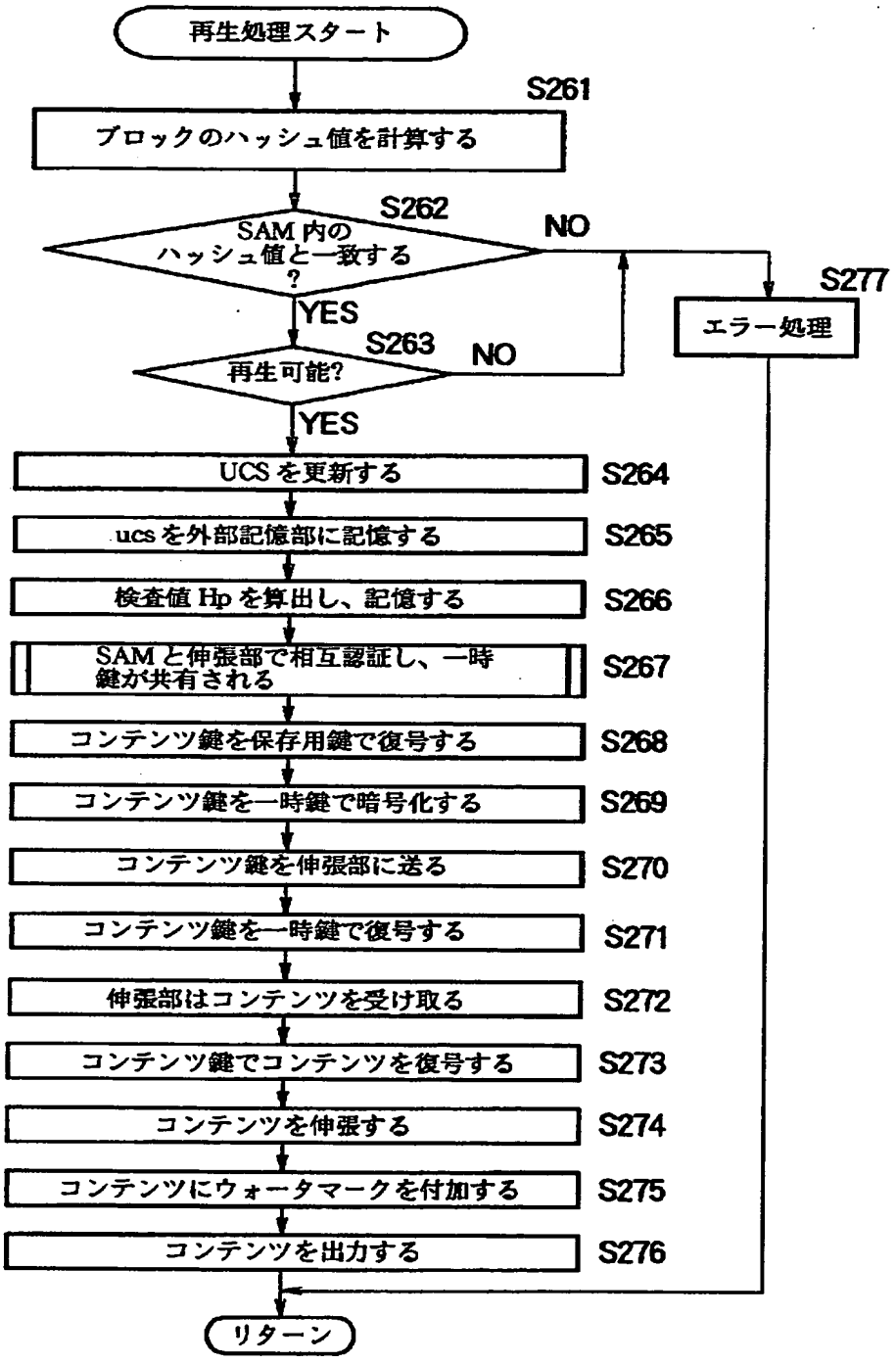
【図３９】


サービスプロバイダセキュアコンテナ供給処理スタート
セキュアコンテナの証明書から公開鍵を取り出す
S221
セキュアコンテナの改竄がないことを確認する
S222
セキュアコンテナからUCPを取り出す
S223
PTを作成
S224
セキュアコンテナを作成
S225
レシーバと相互認証する
S226
セキュアコンテナを送信
S227
リターン

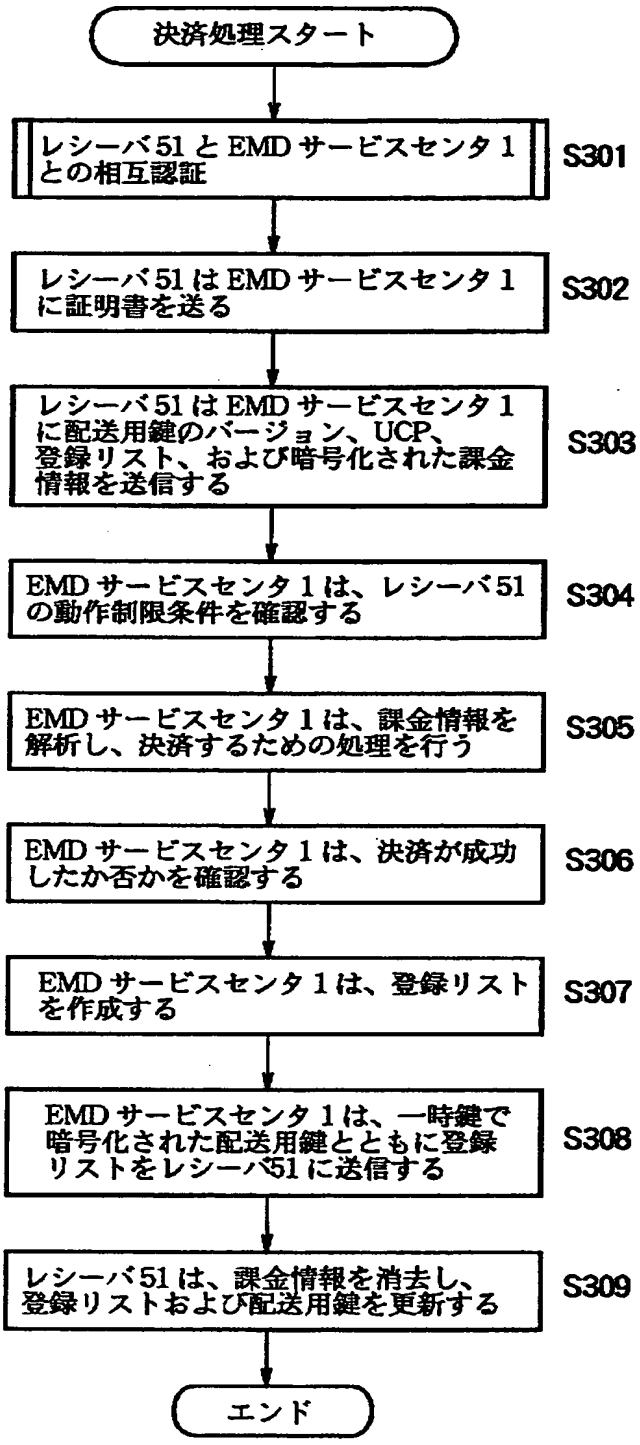
【図４０】


サービスプロバイダセキュアアコンテナの受信の処理スタート
サービスプロバイダから、セキュアコンテナを受信する
S241
サービスプロバイダから、公開鍵証明書を受信する
S242
セキュアコンテナの署名データを検証する
S243
UCPおよびPTを基に利用内容の選択
S244
UCPおよびPTを基に、課金情報およびUCSを作成する
S245
コンテンツをHDDに記録する
S246
コンテンツ鍵を配送用鍵で復号する
S247
コンテンツ鍵を保存用鍵で暗号化する
S248
外部記憶部の空きのあるブロックを検索する
S249
外部記憶部の空きのあるブロックのハッシュ値を計算する
S250
S251
算出したハッシュ値と記憶モジュールの所定の検査値が一致する?
NO
YES
S256
YES
外部記憶部の全てのブロックを調べた?
NO
S257
外部記憶部の空きのある他のブロックを検索する
コンテンツ鍵等を外部記憶部に記憶する
S252
外部記憶部のコンテンツ鍵等を記憶したブロックのハッシュ値を計算する
S253
算出したハッシュ値を記憶モジュールの所定の検査値に上書きする
S254
課金情報を記憶モジュールに記憶する
S255
リターン

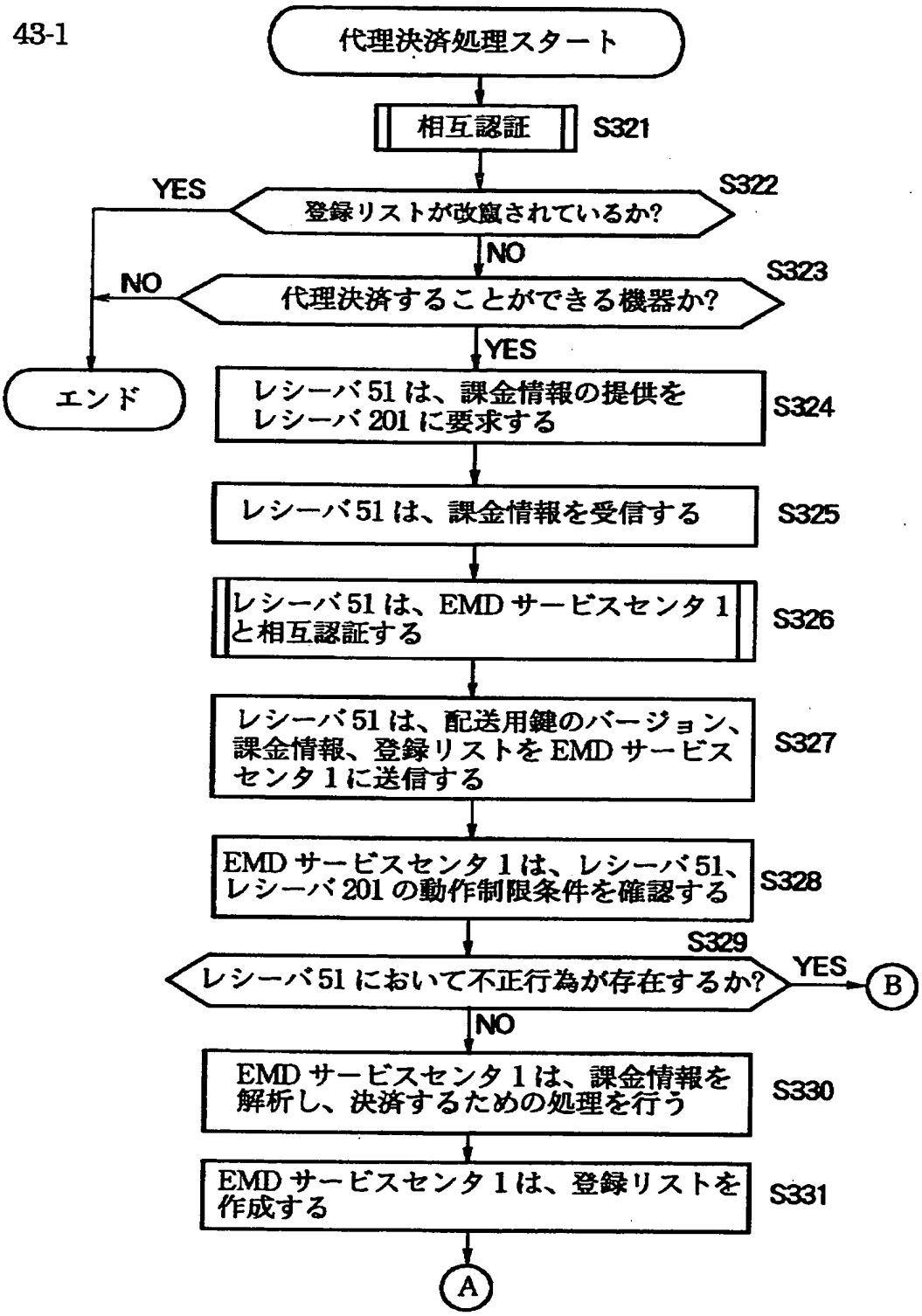
【図４１】


再生処理スタート
S261
ブロックのハッシュ値を計算する
S262
SAM内の
ハッシュ値と一致する
?
NO
S277
エラー処理
YES
S263
再生可能?
NO
YES
UCSを更新する
S264
ucsを外部記憶部に記憶する
S265
検査値Hpを算出し、記憶する
S266
SAMと伸張部で相互認証し、一時
鍵が共有される
S267
コンテンツ鍵を保存用鍵で復号する
S268
コンテンツ鍵を一時鍵で暗号化する
S269
コンテンツ鍵を伸張部に送る
S270
コンテンツ鍵を一時鍵で復号する
S271
伸張部はコンテンツを受け取る
S272
コンテンツ鍵でコンテンツを復号する
S273
コンテンツを伸張する
S274
コンテンツにウォータマークを付加する
S275
コンテンツを出力する
S276
リターン

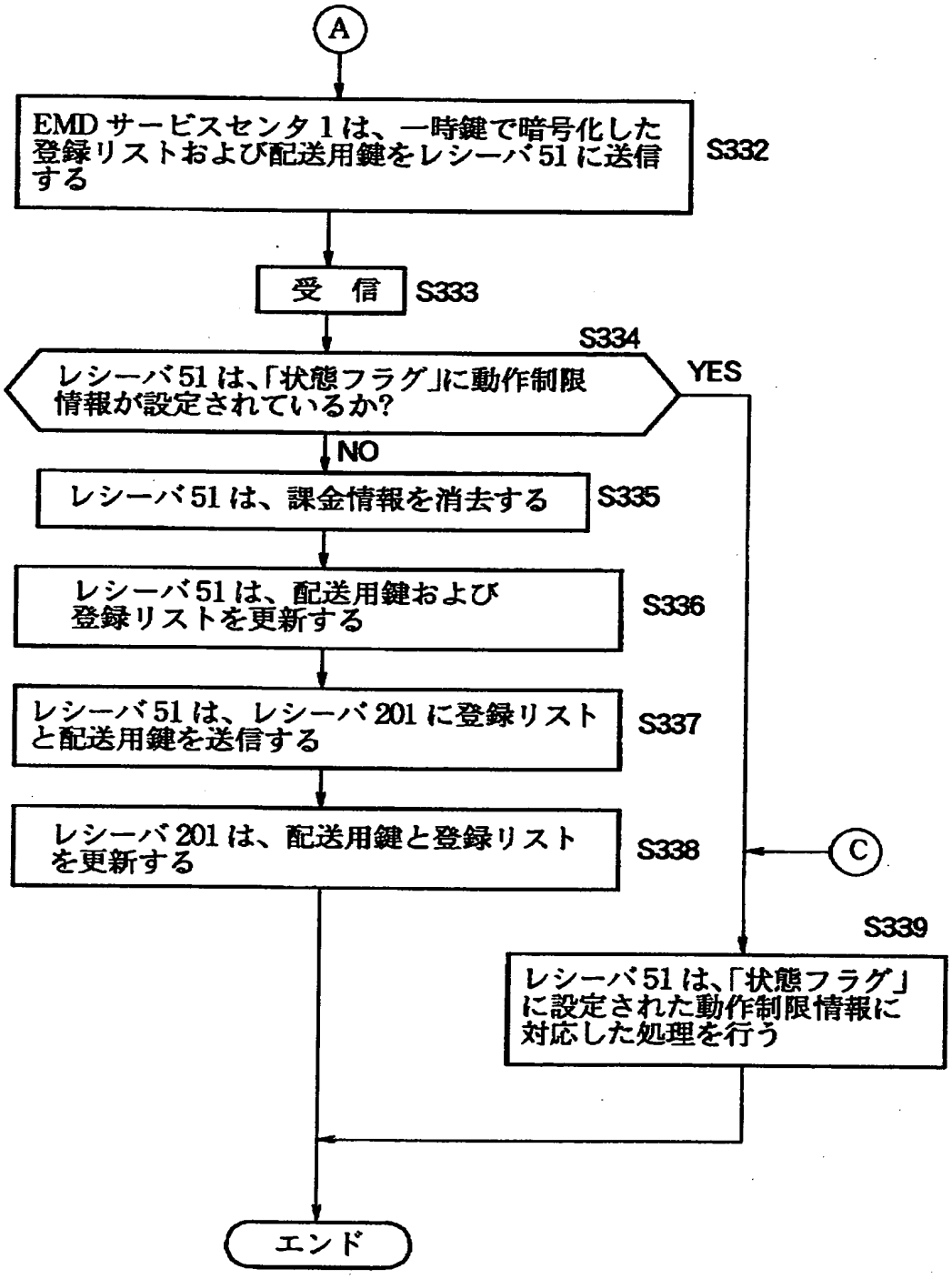
【図４２】


決済処理スタート
レシーバ51とEMDサービスセンタ1との相互認証
S301
レシーバ51はEMDサービスセンタ1に証明書を送る
S302
レシーバ51はEMDサービスセンタ1に配送用鍵のバージョン、UCP、登録リスト、および暗号化された課金情報を送信する
S303
EMDサービスセンタ1は、レシーバ51の動作制限条件を確認する
S304
EMDサービスセンタ1は、課金情報を解析し、決済するための処理を行う
S305
EMDサービスセンタ1は、決済が成功したか否かを確認する
S306
EMDサービスセンタ1は、登録リストを作成する
S307
EMDサービスセンタ1は、一時鍵で暗号化された配送用鍵とともに登録リストをレシーバ51に送信する
S308
レシーバ51は、課金情報を消去し、登録リストおよび配送用鍵を更新する
S309
エンド

【図４３】

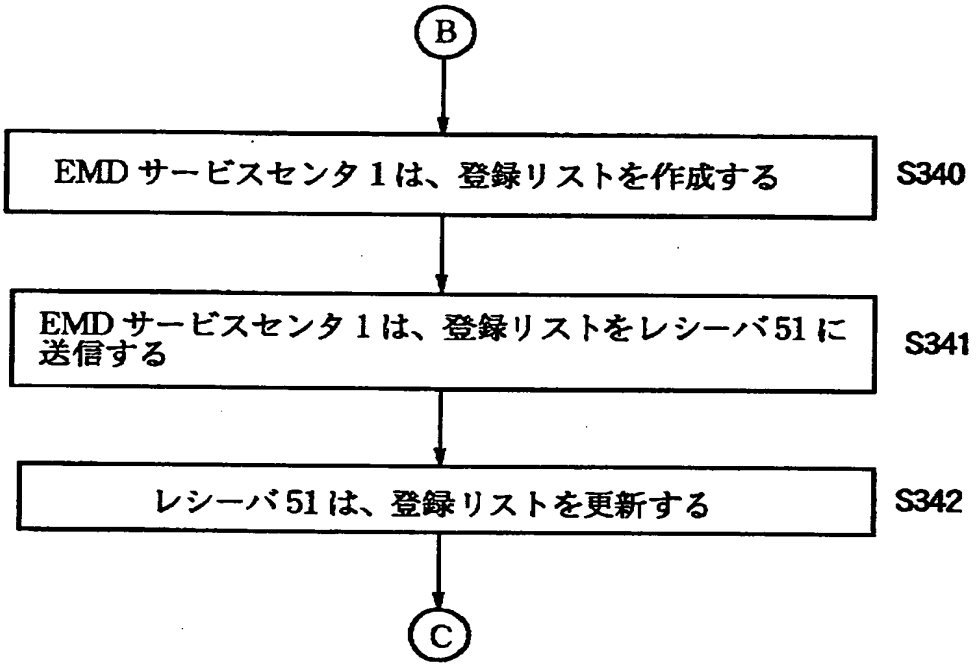

43-1
代理決済処理スタート
相互認証
S321
YES
登録リストが改竄されているか?
S322
NO
NO
代理決済することができる機器か?
S323
YES
エンド
レシーバ51は、課金情報の提供をレシーバ201に要求する
S324
レシーバ51は、課金情報を受信する
S325
レシーバ51は、EMDサービスセンタ1と相互認証する
S326
レシーバ51は、配送用鍵のバージョン、課金情報、登録リストをEMDサービスセンタ1に送信する
S327
EMDサービスセンタ1は、レシーバ51、レシーバ201の動作制限条件を確認する
S328
S329
レシーバ51において不正行為が存在するか?
YES
B
NO
EMDサービスセンタ1は、課金情報を解析し、決済するための処理を行う
S330
EMDサービスセンタ1は、登録リストを作成する
S331
A

【図４４】

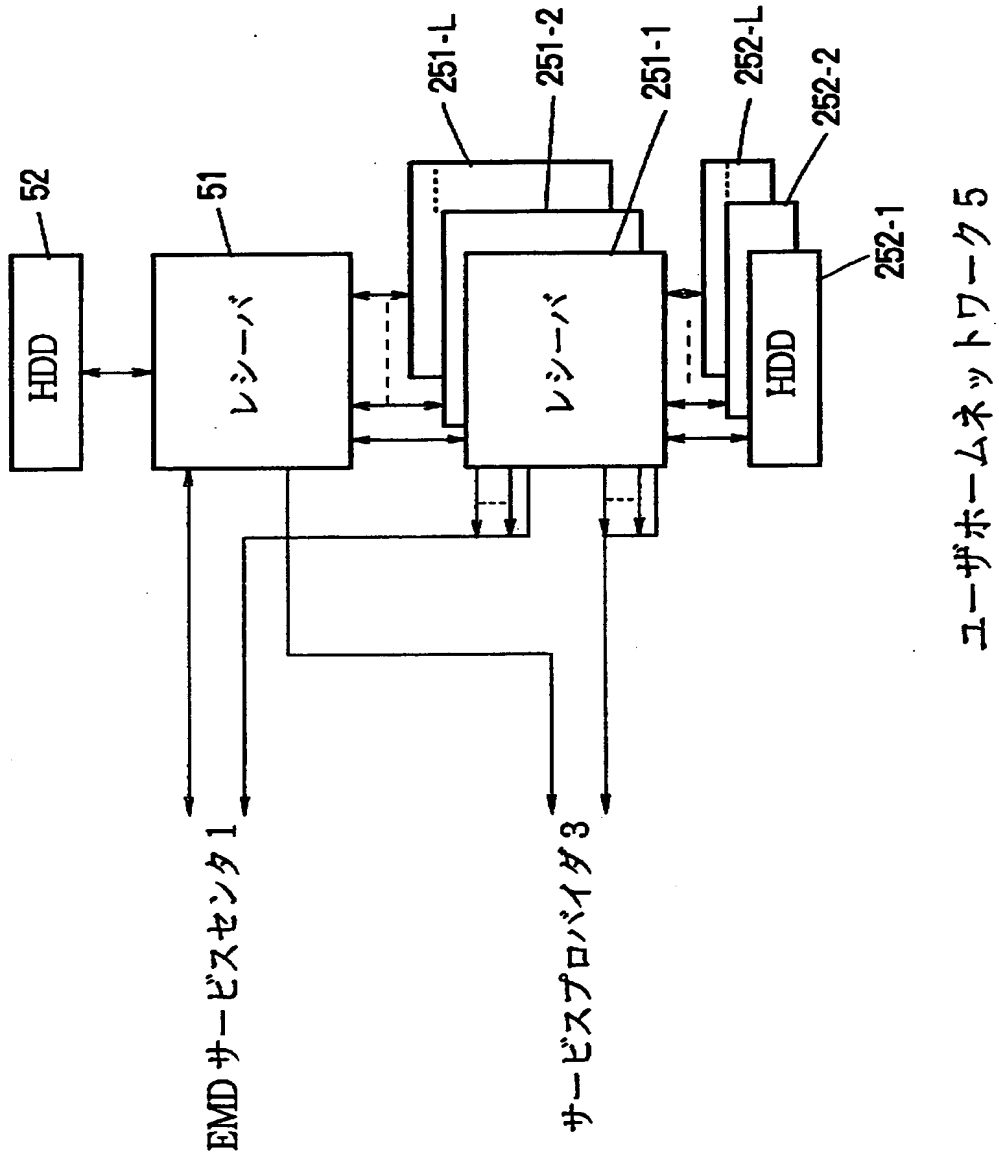

43-2
A
EMDサービスセンタ1は、一時鍵で暗号化した登録リストおよび配送用鍵をレシーバ51に送信する
S332
受　信
S333
S334
レシーバ51は、「状態フラグ」に動作制限情報が設定されているか?
YES
NO
レシーバ51は、課金情報を消去する
S335
レシーバ51は、配送用鍵および登録リストを更新する
S336
レシーバ51は、レシーバ201に登録リストと配送用鍵を送信する
S337
レシーバ201は、配送用鍵と登録リストを更新する
S338
C
S339
レシーバ51は、「状態フラグ」に設定された動作制限情報に対応した処理を行う
エンド

【図４５】

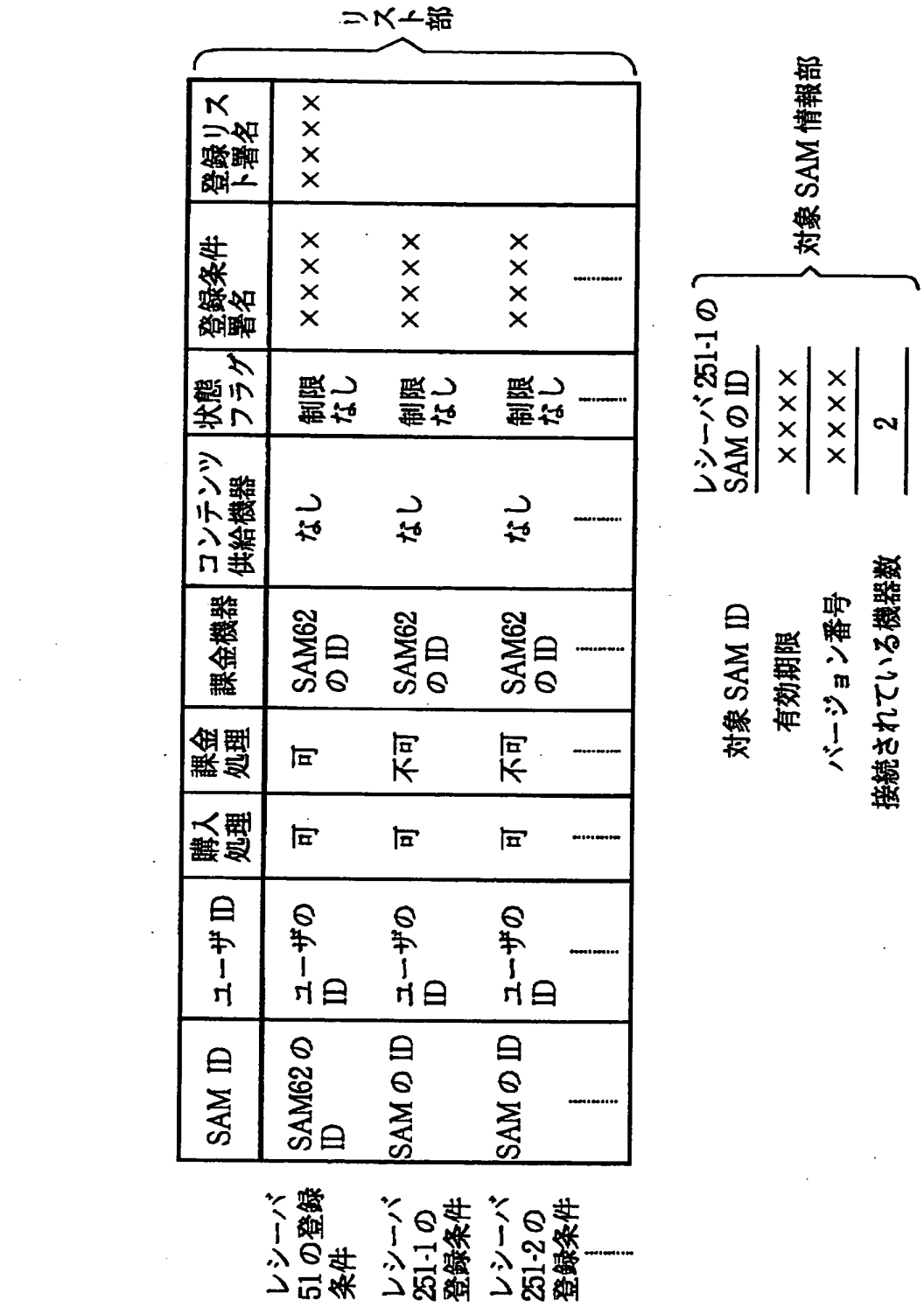
43-3



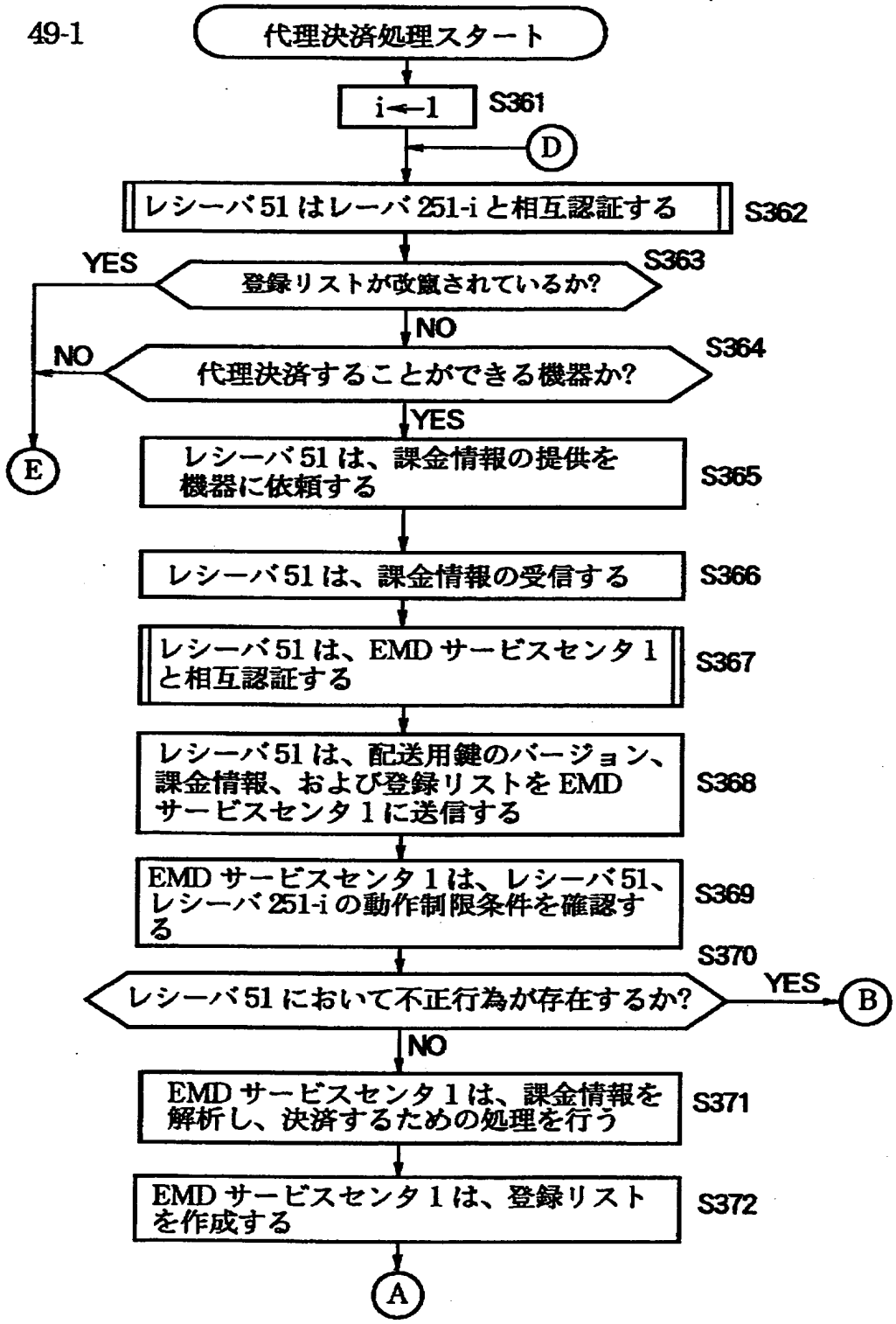
【図４６】


52
51
251-L
251-2
251-1
252-L
252-2
252-1
HDD
レシーバ
レシーバ
HDD
ユーザホームネットワーク５
EMDサービスセンタ１
サービスプロバイダ３

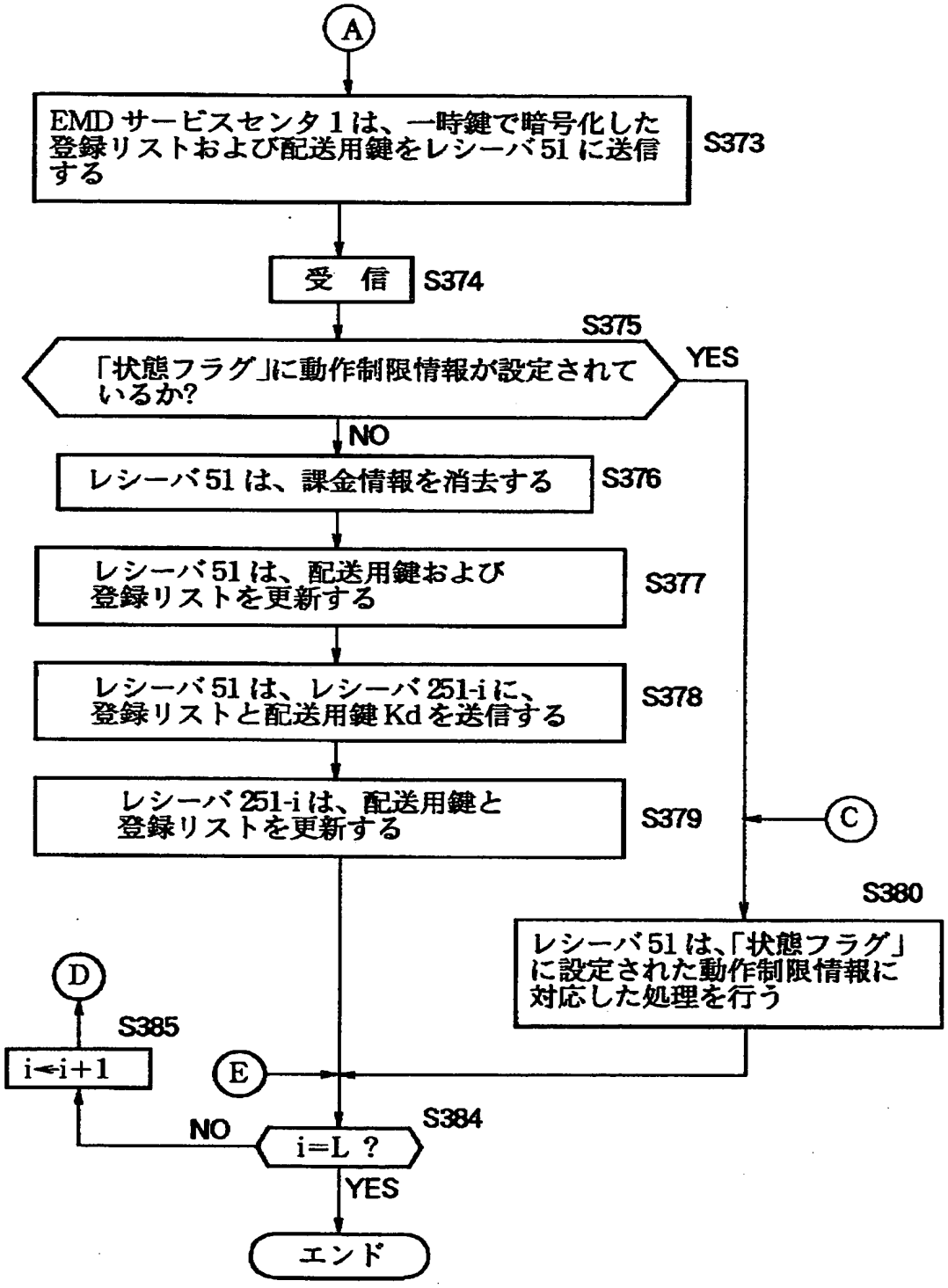
【図４８】


リスト部
SAM ID
ユーザ ID
購入処理
課金処理
課金機器
コンテンツ供給機器
状態フラグ
登録条件署名
登録リスト署名
SAM62のID
ユーザのID
可
可
SAM62のID
なし
制限なし
××××
××××
SAMのID
ユーザのID
不可
不可
SAM62のID
なし
制限なし
××××
SAMのID
ユーザのID
不可
可
SAM62のID
なし
制限なし
××××
レシーバ51の登録条件
レシーバ251-1の登録条件
レシーバ251-2の登録条件
レシーバ251-1のSAMのID
対象SAM ID
有効期限
バージョン番号
接続されている機器数
××××
××××
2
対象SAM情報部

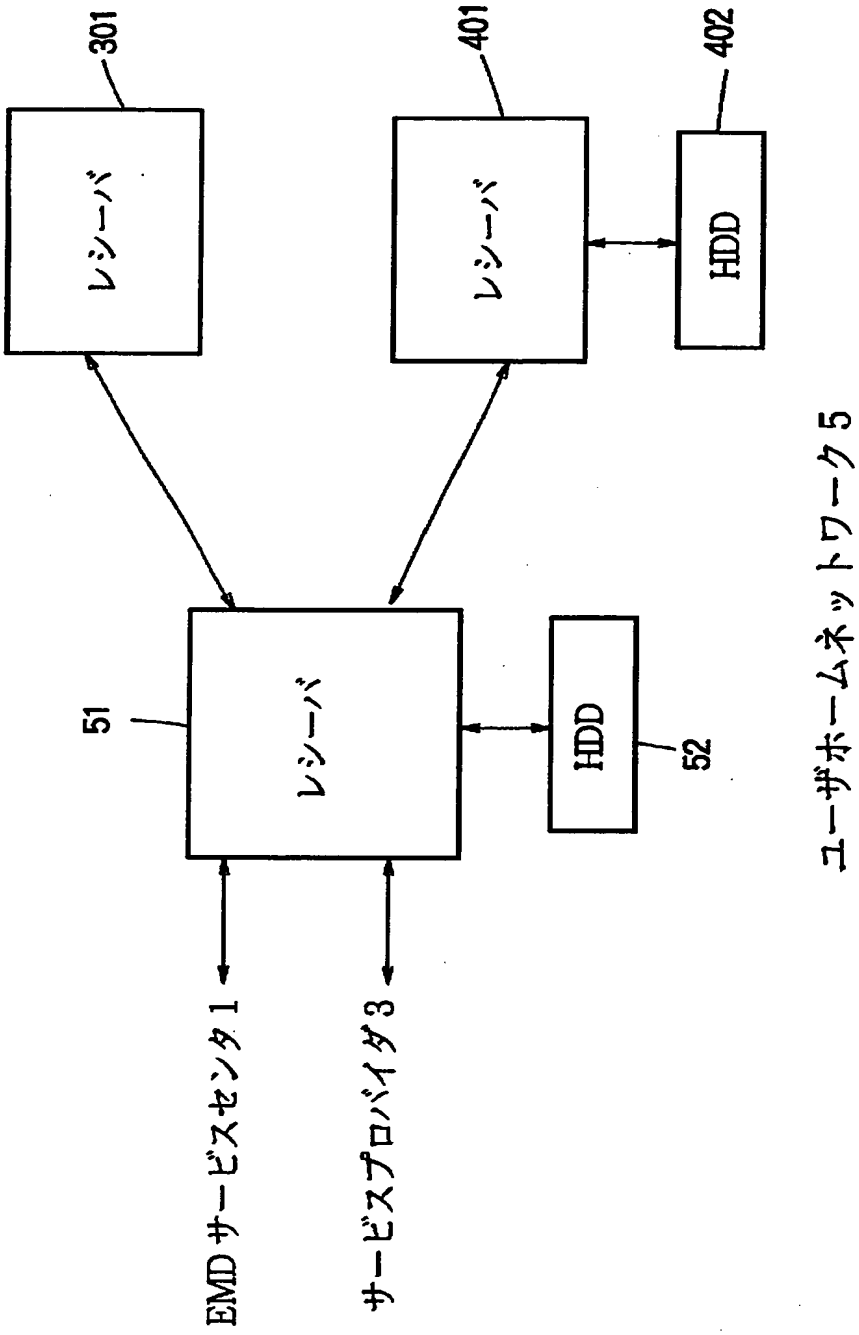
【図４９】


49-1
代理決済処理スタート
i←1
S361
D
レシーバ51はレーバ251-iと相互認証する
S362
YES
登録リストが改竄されているか?
S363
NO
NO
代理決済することができる機器か?
S364
YES
E
レシーバ51は、課金情報の提供を機器に依頼する
S365
レシーバ51は、課金情報の受信する
S366
レシーバ51は、EMDサービスセンタ1と相互認証する
S367
レシーバ51は、配送用鍵のバージョン、課金情報、および登録リストをEMDサービスセンタ1に送信する
S368
EMDサービスセンタ1は、レシーバ51、レシーバ251-iの動作制限条件を確認する
S369
S370
レシーバ51において不正行為が存在するか?
YES
B
NO
EMDサービスセンタ1は、課金情報を解析し、決済するための処理を行う
S371
EMDサービスセンタ1は、登録リストを作成する
S372
A

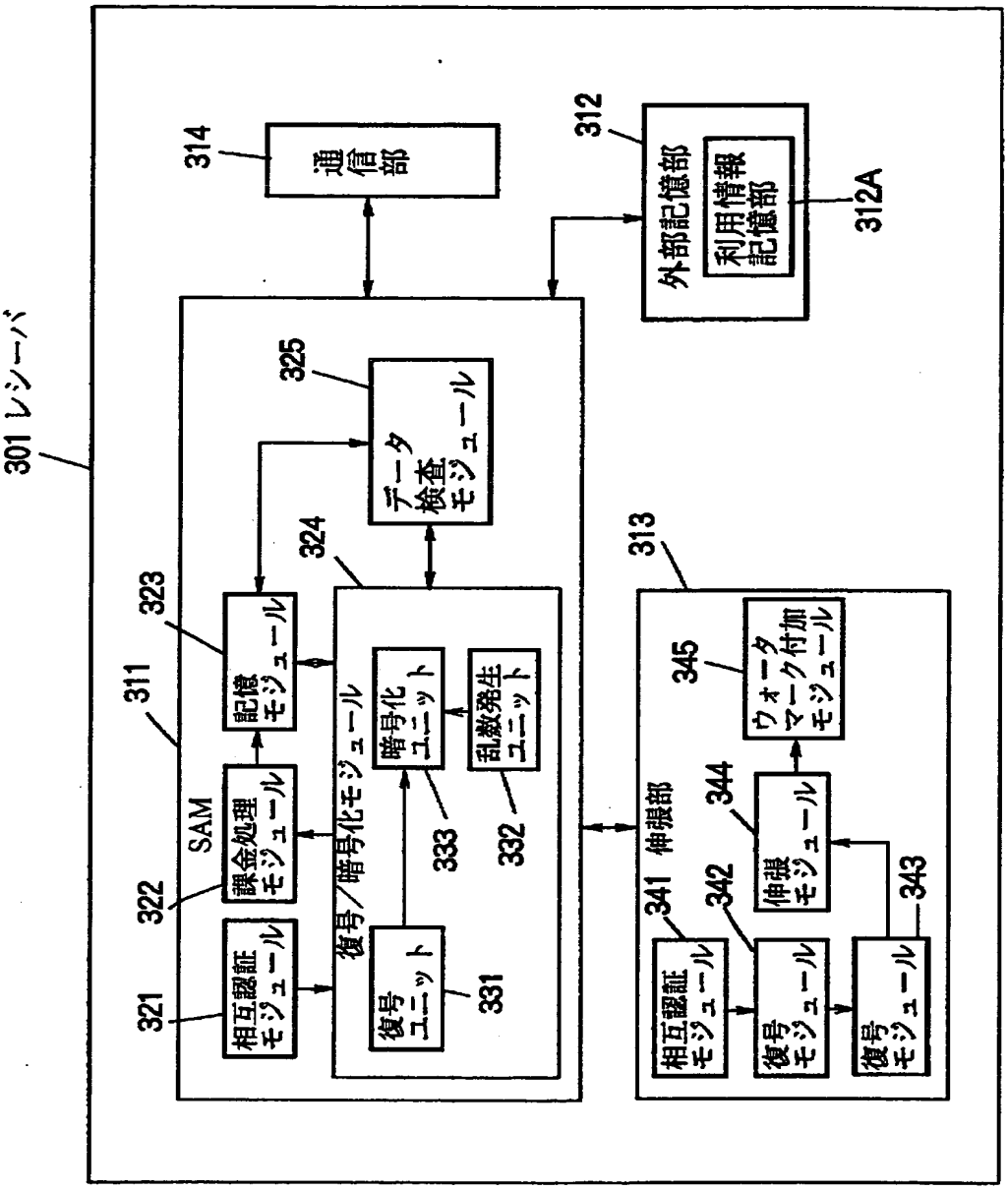
【図５０】


49-2
A
EMDサービスセンタ1は、一時鍵で暗号化した登録リストおよび配送用鍵をレシーバ51に送信する
S373
受　信
S374
S375
「状態フラグ」に動作制限情報が設定されているか?
YES
NO
レシーバ51は、課金情報を消去する
S376
レシーバ51は、配送用鍵および登録リストを更新する
S377
レシーバ51は、レシーバ251-iに、登録リストと配送用鍵Kdを送信する
S378
レシーバ251-iは、配送用鍵と登録リストを更新する
S379
C
S380
レシーバ51は、「状態フラグ」に設定された動作制限情報に対応した処理を行う
D
S385
i←i+1
E
NO
S384
i=L ?
YES
エンド

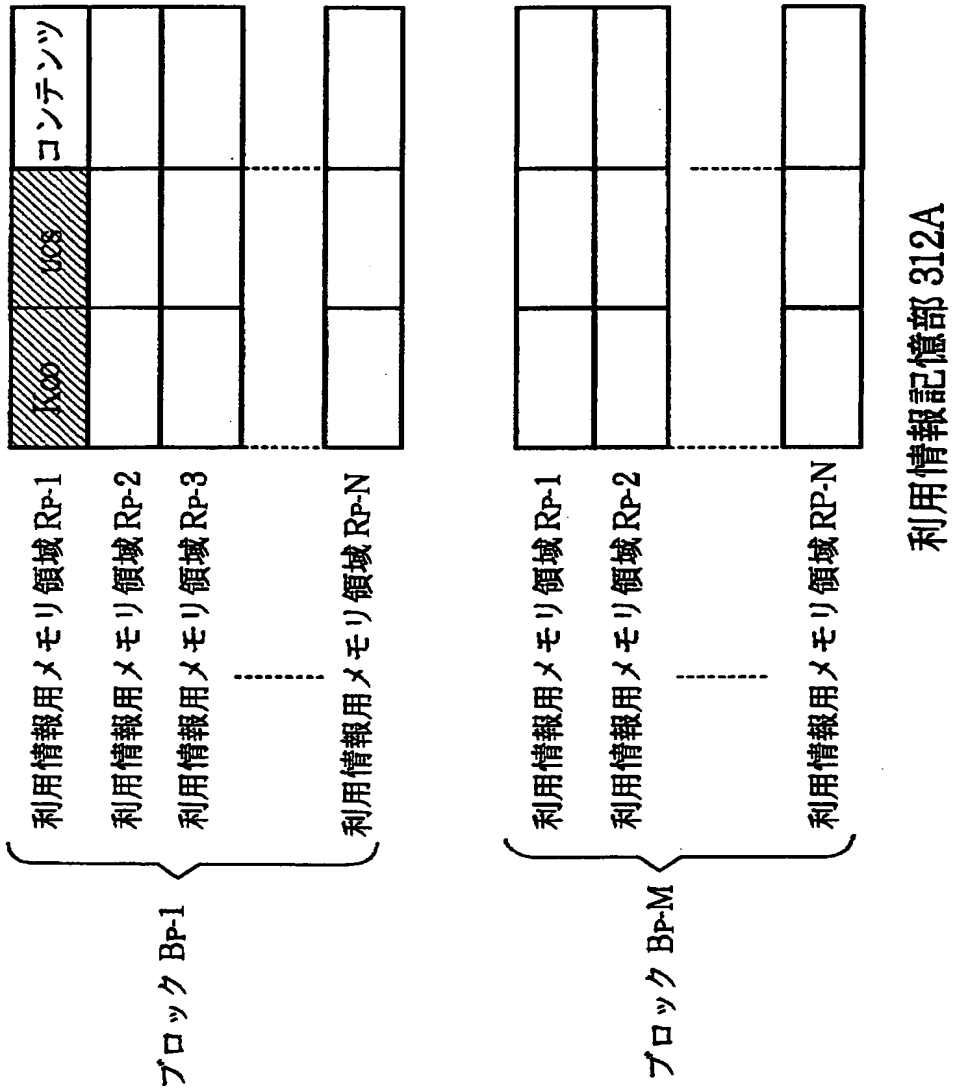
【図５２】


301
401
402
レシーバ
レシーバ
HDD
51
レシーバ
HDD
52
ユーザホームネットワーク５
EMDサービスセンタ１
サービスプロバイダ３

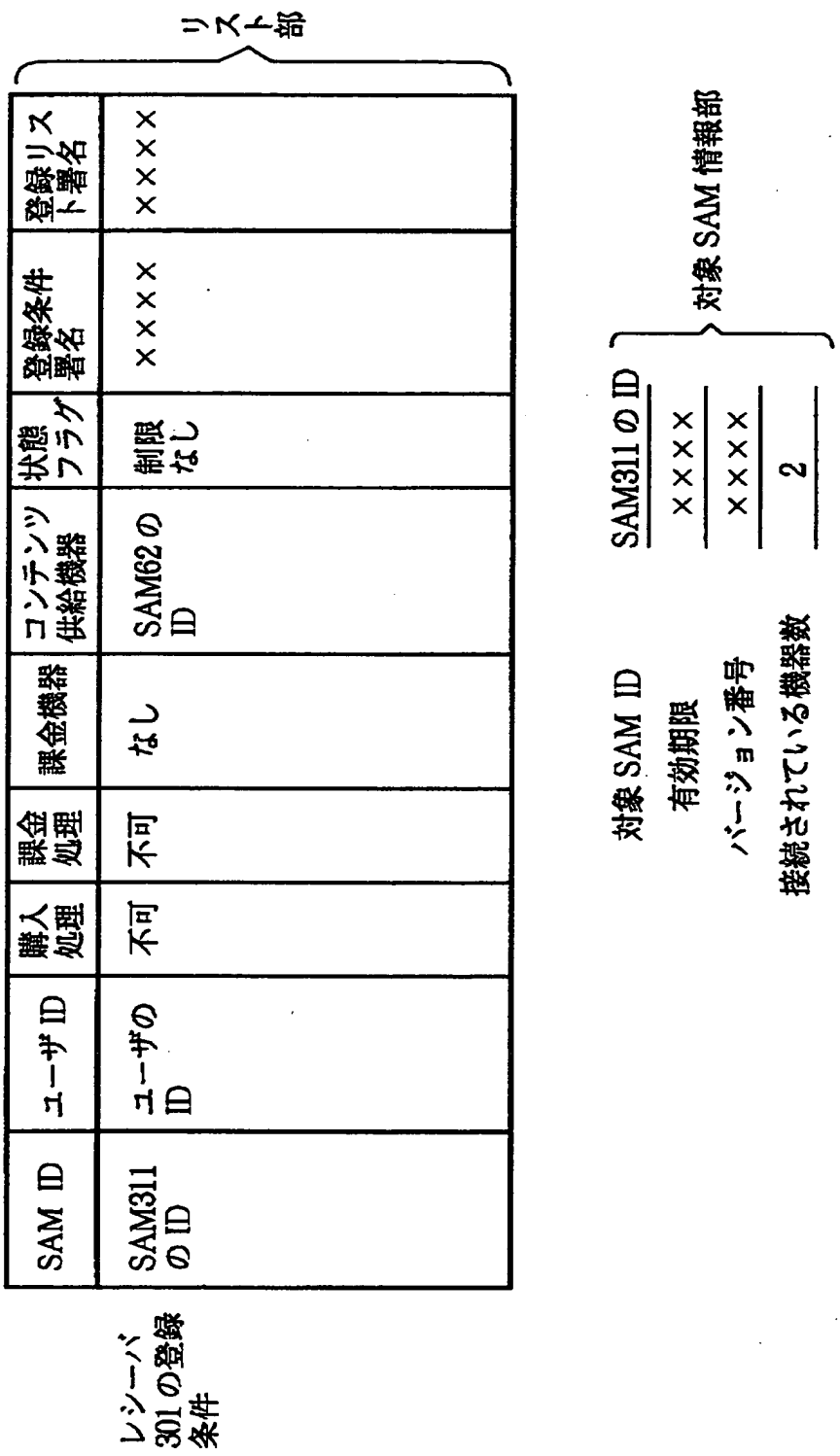
【図５３】


301 レシーバ
314
通信部
312
外部記憶部
利用情報記憶部
312A
325
データ検査モジュール
324
313
311
323
記憶モジュール
345
ウォータマーク付加モジュール
SAM
課金処理モジュール
322
暗号化ユニット
乱数発生ユニット
333
332
復号／暗号化モジュール
344
伸張モジュール
341 伸張部
342
343
相互認証モジュール
321
復号ユニット
331
相互認証モジュール
復号モジュール
復号モジュール

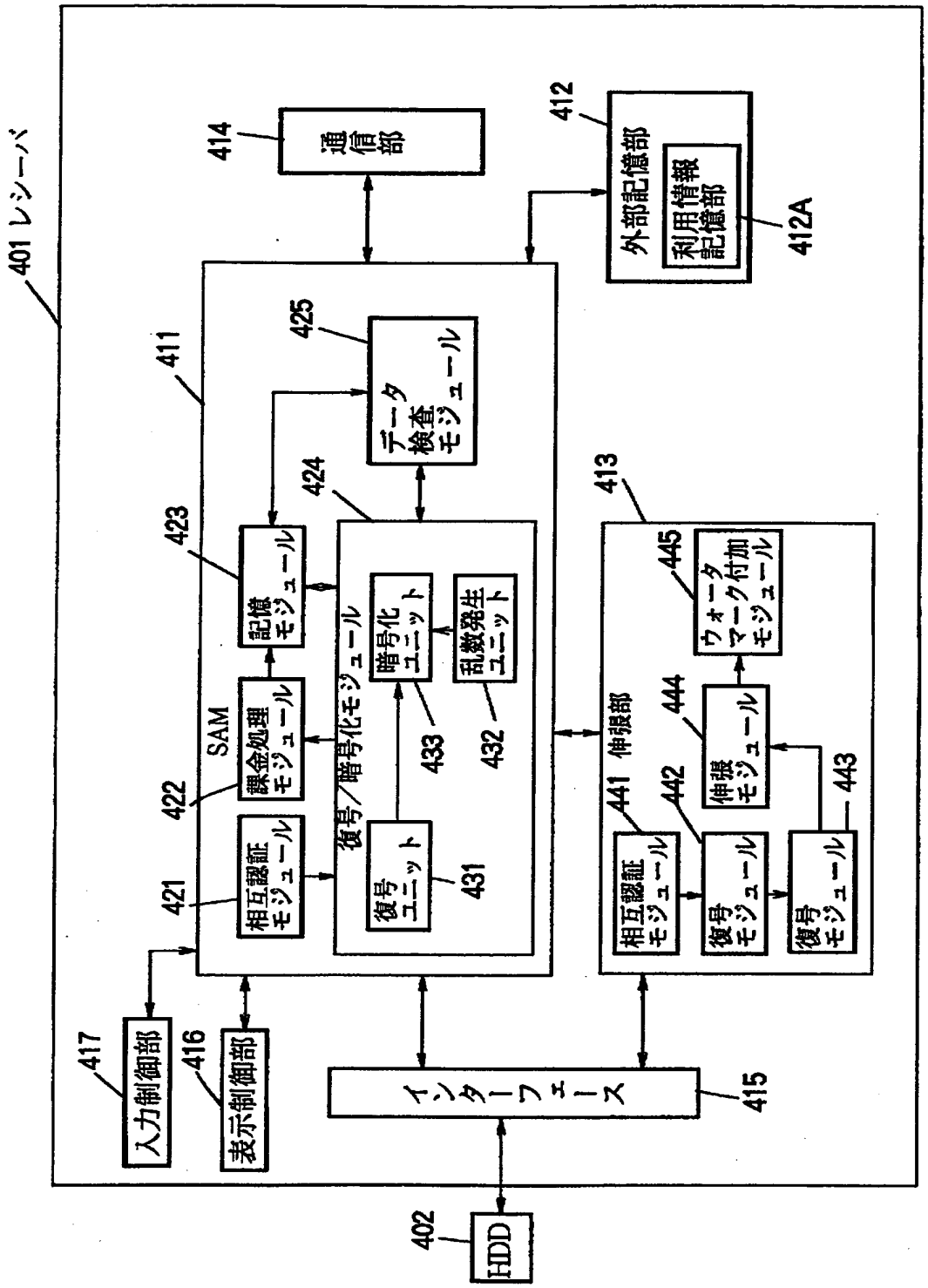
【図５４】


Kos
OS
コンテンツ
利用情報用メモリ領域 Rp-1
利用情報用メモリ領域 Rp-2
利用情報用メモリ領域 Rp-3
利用情報用メモリ領域 Rp-N
ブロック Bp-1
利用情報用メモリ領域 Rp-1
利用情報用メモリ領域 Rp-2
利用情報用メモリ領域 RP-N
ブロック Bp-M
利用情報記憶部 312A

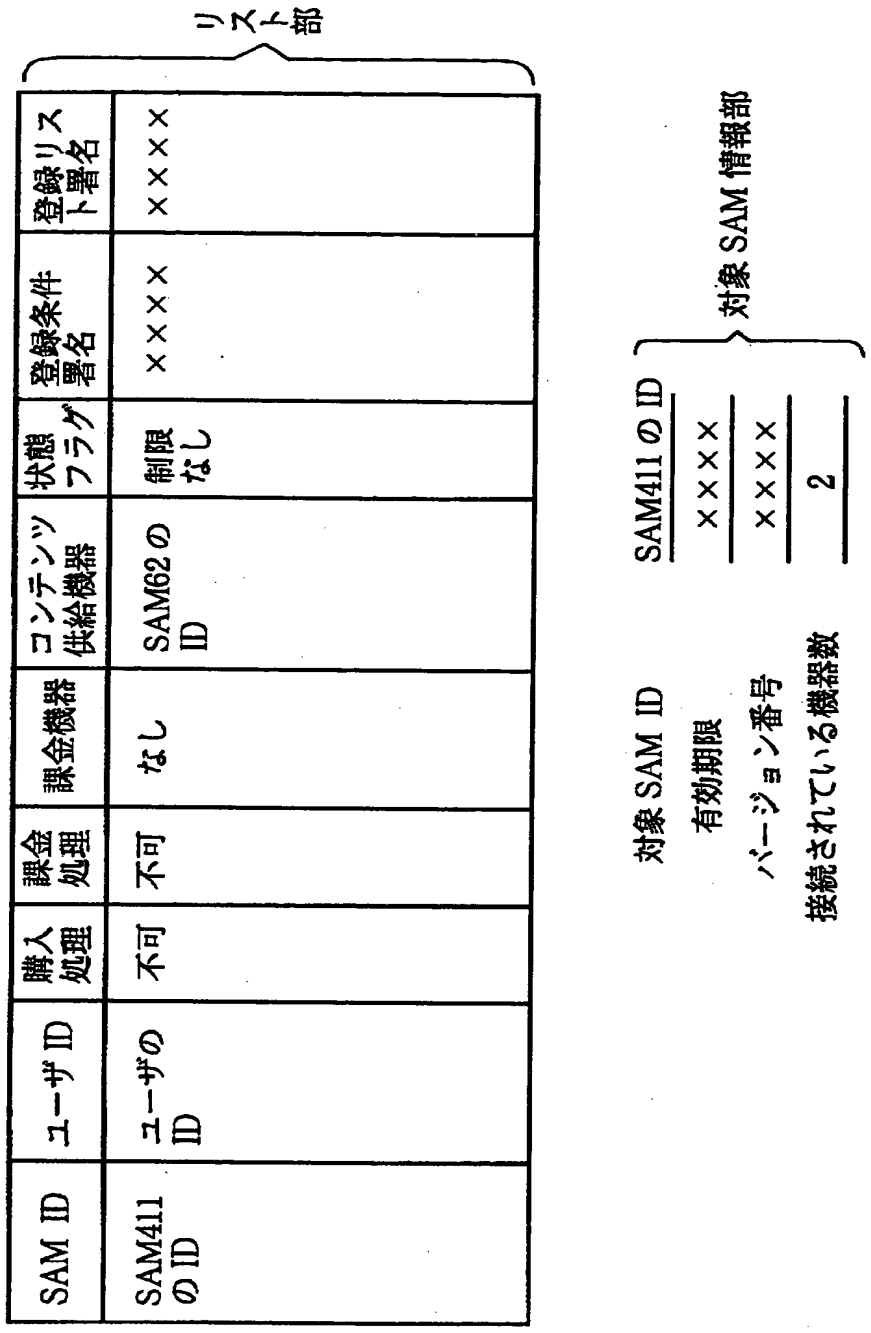
【図５５】


リスト部
SAM ID
ユーザ ID
購入処理
課金処理
課金機器
コンテンツ供給機器
状態フラグ
登録条件署名
登録リスト署名
SAM311のID
ユーザのID
不可
不可
なし
SAM62のID
制限なし
××××
××××
レシーバ301の登録条件
対象SAM ID
有効期限
バージョン番号
接続されている機器数
SAM311のID
××××
××××
2
対象SAM情報部
レシーバ301の登録リスト

【図５６】


401 レシーバ
414 通信部
412 外部記憶部
利用情報記憶部
412A
411
425 データ検査モジュール
424
423 記憶モジュール
暗号化ユニット
乱数発生ユニット
433
432
SAM
課金処理モジュール
422
復号／暗号化モジュール
413
445 ウォータマーク付加モジュール
444 伸張モジュール
441 伸張部
442
443
相互認証モジュール
421
復号ユニット
431
復号モジュール
復号モジュール
417 入力制御部
416 表示制御部
インターフェース
415
402 HDD

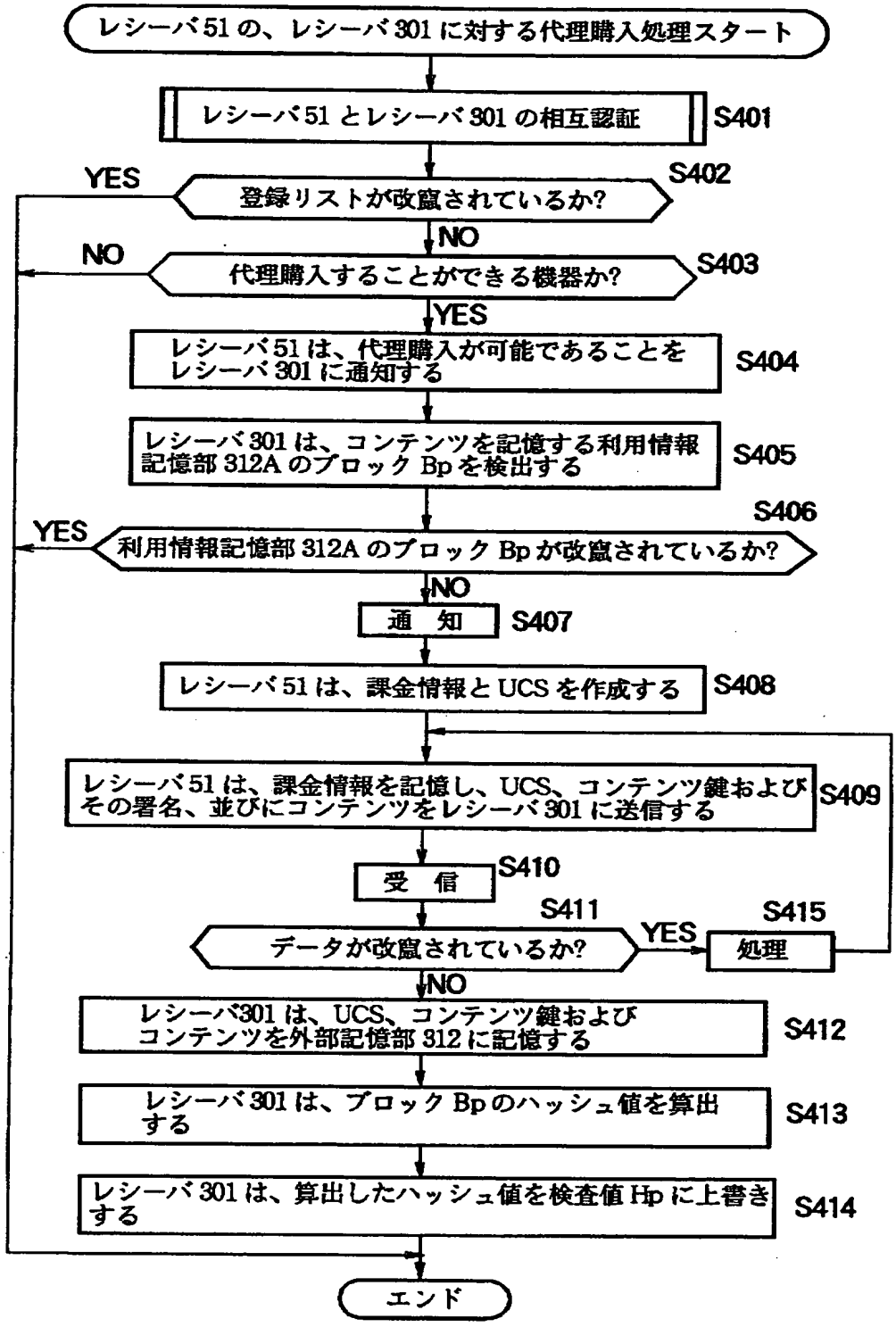
【図５７】


リスト部
SAM ID
ユーザ ID
購入処理
課金処理
課金機器
コンテンツ供給機器
状態フラグ
登録条件署名
登録リスト署名
SAM411のID
ユーザのID
不可
不可
なし
SAM62のID
制限なし
××××
××××
レシーバ401の登録条件
対象SAM ID
SAM411のID
有効期限
××××
バージョン番号
××××
接続されている機器数
2
対象SAM情報部
レシーバ401の登録リスト

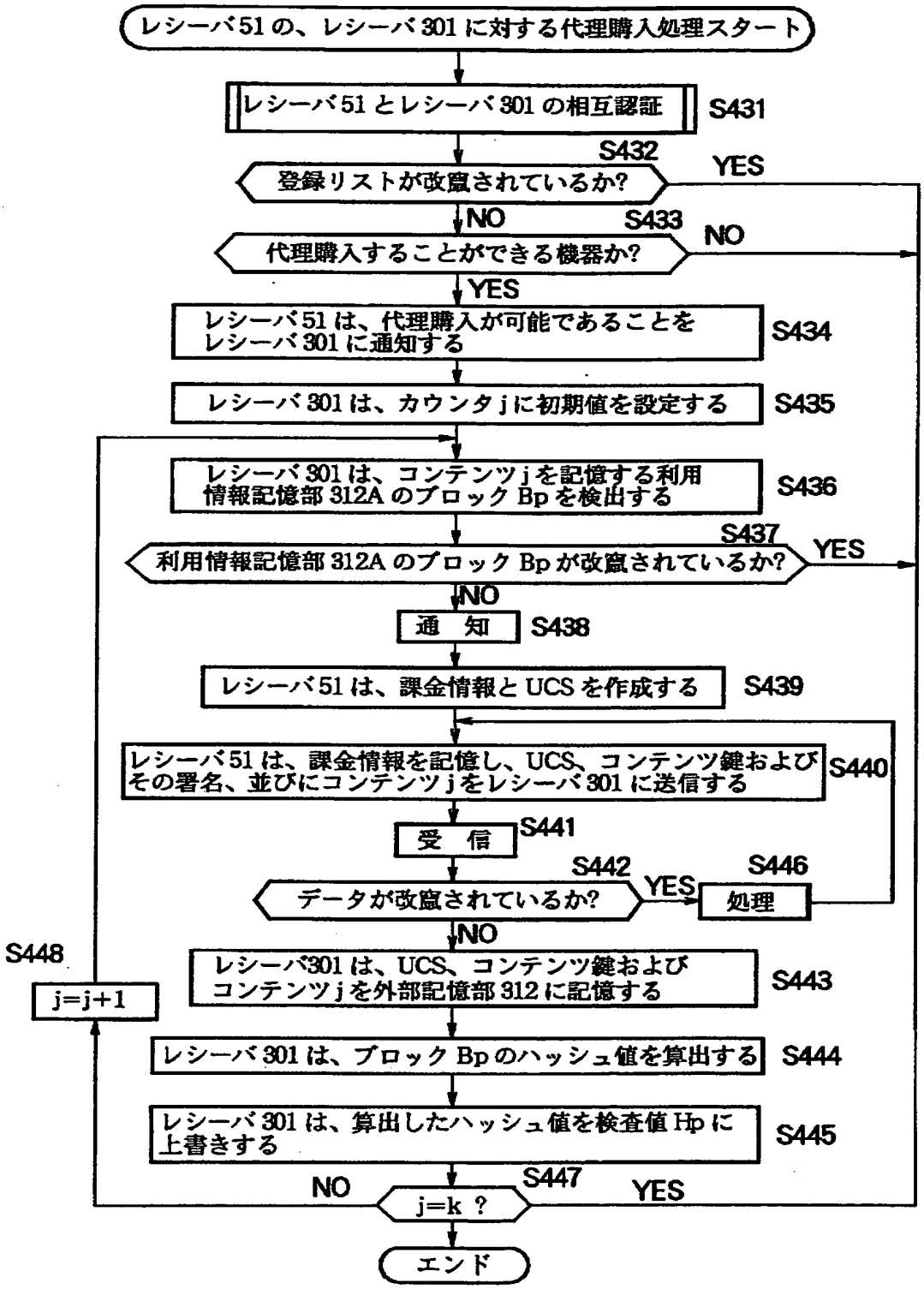
【図５８】

リスト部
SAM ID
ユーザ ID
購入処理
課金処理
課金機器
コンテンツ供給機器
状態フラグ
登録条件署名
登録リスト署名
SAM62のID
ユーザのID
可
可
SAM62のID
なし
制限なし
××××
××××
SAM311のID
ユーザのID
不可
不可
なし
SAM62のID
制限なし
××××
SAM411のID
ユーザのID
不可
不可
なし
SAM62のID
制限なし
××××
レシーバ51の登録条件
レシーバ301の登録条件
レシーバ401の登録条件
対象SAM ID
SAM62のID
有効期限
××××
バージョン番号
××××
接続されている機器数
3
対象SAM情報部
登録リスト

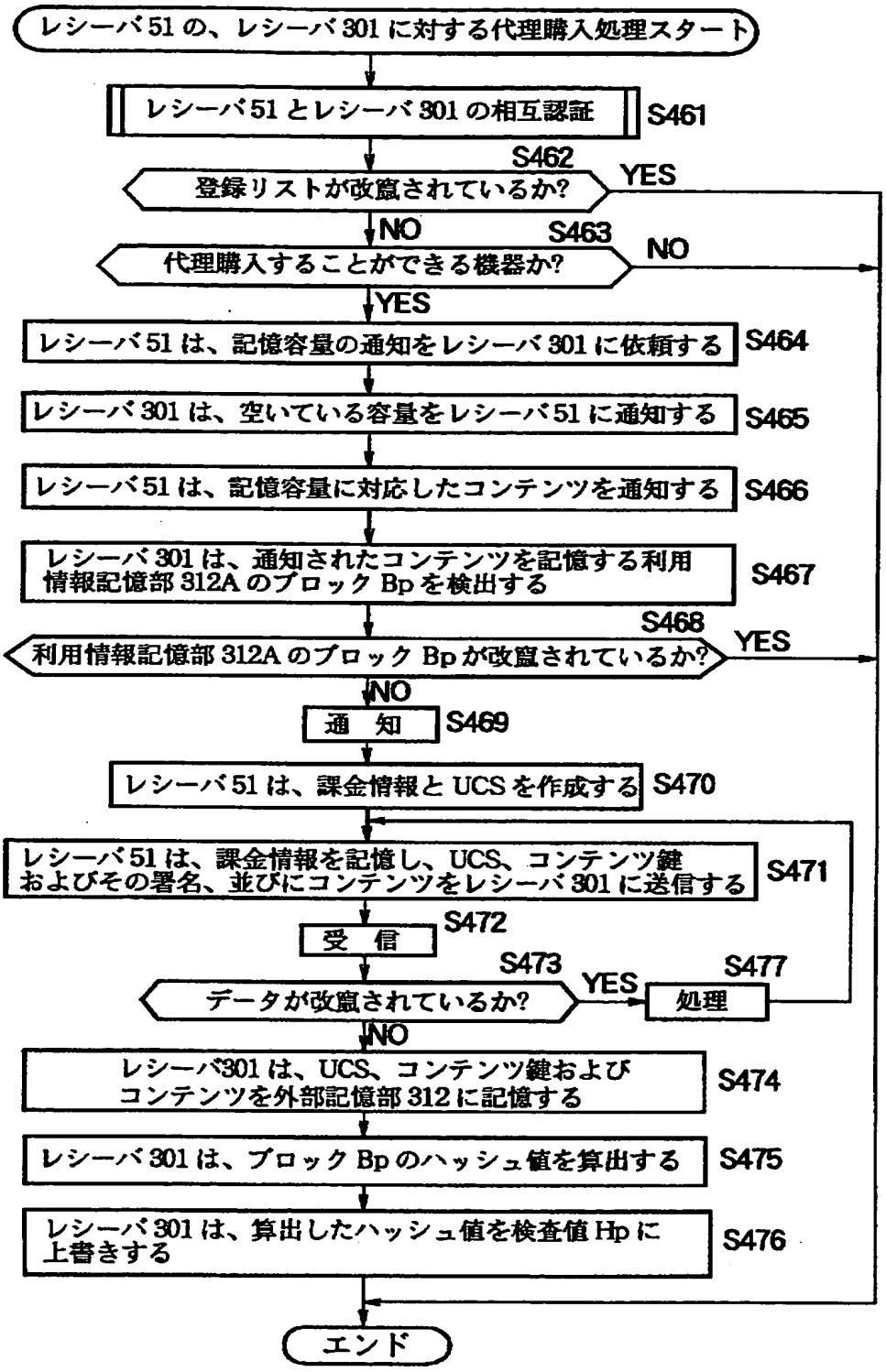
【図５９】


レシーバ51の、レシーバ301に対する代理購入処理スタート
レシーバ51とレシーバ301の相互認証
S401
YES
登録リストが改竄されているか?
S402
NO
NO
代理購入することができる機器か?
S403
YES
レシーバ51は、代理購入が可能であることを
レシーバ301に通知する
S404
レシーバ301は、コンテンツを記憶する利用情報
記憶部312Aのブロック Bpを検出する
S405
S406
YES
利用情報記憶部312Aのブロック Bpが改竄されているか?
NO
通　知
S407
レシーバ51は、課金情報とUCSを作成する
S408
レシーバ51は、課金情報を記憶し、UCS、コンテンツ鍵および
その署名、並びにコンテンツをレシーバ301に送信する
S409
受　信
S410
S411
S415
データが改竄されているか?
YES
処理
NO
レシーバ301は、UCS、コンテンツ鍵および
コンテンツを外部記憶部312に記憶する
S412
レシーバ301は、ブロック Bpのハッシュ値を算出
する
S413
レシーバ301は、算出したハッシュ値を検査値 Hpに上書き
する
S414
エンド

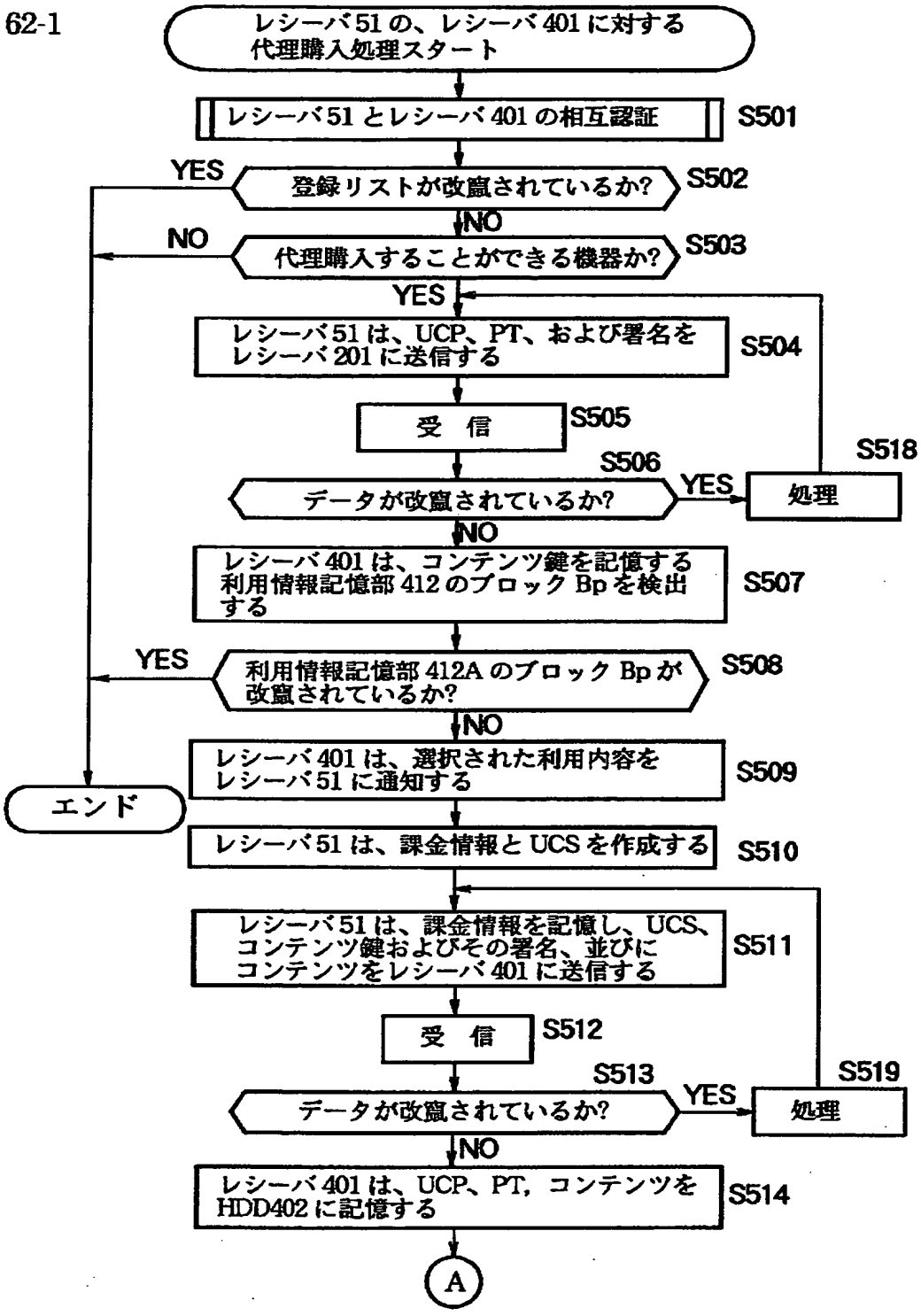
【図６０】


レシーバ51の、レシーバ301に対する代理購入処理スタート
レシーバ51とレシーバ301の相互認証
S431
S432
登録リストが改竄されているか?
YES
NO
S433
代理購入することができる機器か?
NO
YES
レシーバ51は、代理購入が可能であることを
レシーバ301に通知する
S434
レシーバ301は、カウンタjに初期値を設定する
S435
レシーバ301は、コンテンツjを記憶する利用
情報記憶部312Aのブロック Bpを検出する
S436
S437
利用情報記憶部312Aのブロック Bpが改竄されているか?
YES
NO
通　知
S438
レシーバ51は、課金情報とUCSを作成する
S439
レシーバ51は、課金情報を記憶し、UCS、コンテンツ鍵および
その署名、並びにコンテンツjをレシーバ301に送信する
S440
受　信
S441
S442
データが改竄されているか?
YES
S446
処理
NO
S448
j=j+1
レシーバ301は、UCS、コンテンツ鍵および
コンテンツjを外部記憶部312に記憶する
S443
レシーバ301は、ブロック Bpのハッシュ値を算出する
S444
レシーバ301は、算出したハッシュ値を検査値 Hpに
上書きする
S445
NO
S447
j=k ?
YES
エンド

【図６１】

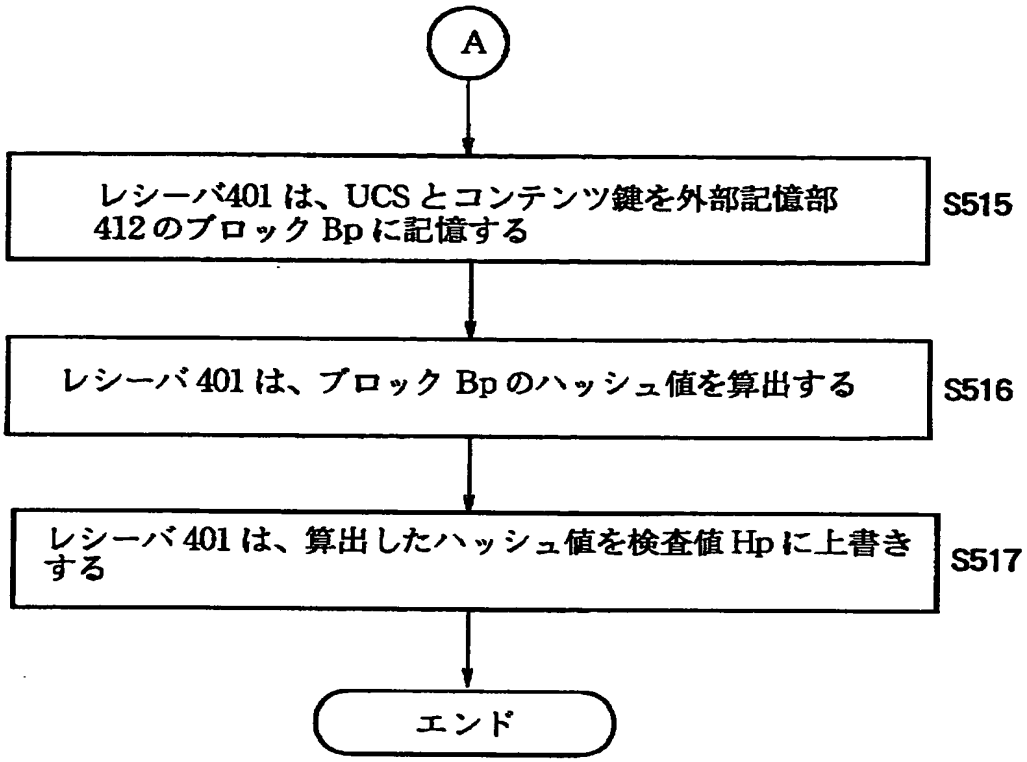

レシーバ51の、レシーバ301に対する代理購入処理スタート
レシーバ51とレシーバ301の相互認証
S461
S462
登録リストが改竄されているか?
YES
NO
S463
代理購入することができる機器か?
NO
YES
レシーバ51は、記憶容量の通知をレシーバ301に依頼する
S464
レシーバ301は、空いている容量をレシーバ51に通知する
S465
レシーバ51は、記憶容量に対応したコンテンツを通知する
S466
レシーバ301は、通知されたコンテンツを記憶する利用情報記憶部312Aのブロック Bpを検出する
S467
S468
利用情報記憶部312Aのブロック Bpが改竄されているか?
YES
NO
通　知
S469
レシーバ51は、課金情報とUCSを作成する
S470
レシーバ51は、課金情報を記憶し、UCS、コンテンツ鍵およびその署名、並びにコンテンツをレシーバ301に送信する
S471
受　信
S472
S473
データが改竄されているか?
YES
S477
処理
NO
レシーバ301は、UCS、コンテンツ鍵およびコンテンツを外部記憶部312に記憶する
S474
レシーバ301は、ブロック Bpのハッシュ値を算出する
S475
レシーバ301は、算出したハッシュ値を検査値 Hpに上書きする
S476
エンド

【図６２】


62-1
レシーバ51の、レシーバ401に対する代理購入処理スタート
レシーバ51とレシーバ401の相互認証
S501
YES
登録リストが改竄されているか?
S502
NO
NO
代理購入することができる機器か?
S503
YES
レシーバ51は、UCP、PT、および署名をレシーバ201に送信する
S504
受　信
S505
S506
データが改竄されているか?
YES
S518
処理
NO
レシーバ401は、コンテンツ鍵を記憶する利用情報記憶部412のブロックBpを検出する
S507
YES
利用情報記憶部412Aのブロック Bpが改竄されているか?
S508
NO
レシーバ401は、選択された利用内容をレシーバ51に通知する
S509
エンド
レシーバ51は、課金情報とUCSを作成する
S510
レシーバ51は、課金情報を記憶し、UCS、コンテンツ鍵およびその署名、並びにコンテンツをレシーバ401に送信する
S511
受　信
S512
S513
データが改竄されているか?
YES
S519
処理
NO
レシーバ401は、UCP、PT，コンテンツをHDD402に記憶する
S514
A

【図６３】

62-2


A
レシーバ401は、UCSとコンテンツ鍵を外部記憶部412のブロックBpに記憶する
S515
レシーバ401は、ブロックBpのハッシュ値を算出する
S516
レシーバ401は、算出したハッシュ値を検査値Hpに上書きする
S517
エンド

【書類名】　　要約書

【要約】

【課題】　主の情報処理装置が、それに接続される情報処理装置に代わって、課金を決済する処理を行うことができるようにする。

【解決手段】　課金を決済する処理を行うことができないレシーバ２０１に代わって、レシーバ２０１において計上された課金を決済する処理を、レシーバ５１が行う。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社